U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5048

Proposed Revision 2 to Regulatory Guide 5.54

Issue Date: May 2018
Technical Lead: Dennis Gordon

STANDARD FORMAT AND CONTENT OF PHYSICAL SECURITY PLANS, TRAINING AND QUALIFICATION PLANS, AND SAFEGUARDS CONTINGENCY PLANS FOR NUCLEAR POWER PLANTS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes the standard format and content for licensee physical security plans, training and qualification plans, and safeguards contingency plans that the U.S. Nuclear Regulatory Commission (NRC) staff finds acceptable. Collectively, these three plans (along with the licensee cyber security plan) are referred to as security plans. This RG provides general guidance for the level of detail that licensees should provide in these plans relative to the types of information that should be addressed, including site-specific conditions, to ensure that security plans are complete and accurate.

An acceptable physical security plan describes how the licensee will implement the Commission's requirements set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials," Section 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage" (Ref. 1). An acceptable training and qualification plan describes how the licensee will implement the Commission's requirements set forth in 10 CFR Part 73, Appendix B, Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties." An acceptable safeguards contingency plan describes how the licensee will implement the Commission's requirements set forth in 10 CFR Part 73, Appendix C, Section II, "Nuclear Power Plant Safeguards Contingency Plans." An acceptable cyber security plan describes how the licensee will implement the Commission's requirements set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." Specific guidance pertaining to the standard format and content for Cyber Security Plans is not discussed in this RG, but can be found in RG 5.71, "Cyber Security Programs for Nuclear Facilities" and Nuclear Energy Institute (NEI) guidance NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors."

Applicability

This RG provides guidance for nuclear power reactor applicants and licensees under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 2), and under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 3). New reactor applicants should consider this guidance in preparing an application for a combined license (COL) under 10 CFR Part 52. This guide specifically provides guidance to licensees that are required to have a physical security plan, a safeguards contingency plan, and a training and qualification plan under 10 CFR 73.55(c).

In addition, the guidance in this RG is applicable to nuclear power reactor licensees that operate an independent spent fuel storage installation (ISFSI) under the general license issued by 10 CFR 72.210, "General license issued under § 72.210" (Ref. 4). General license ISFSIs are subject to the physical protection requirements of 10 CFR 73.55, with specific additional conditions and exceptions enumerated in 10 CFR 72.212(b)(9).

Finally, this RG may be considered for use by licensees and applicants for an ISFSI operated in accordance with a specific license issued under 10 CFR 72.40, "Issuance of license," and subject to the requirements of 10 CFR 72.180, "Physical protection plan," and 10 CFR 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste." The physical protection requirements applicable to specific license ISFSIs have many similarities with the physical protection requirements for general license ISFSIs. Accordingly, licensees and applicants for a specific license ISFSI may consider the guidance provided in this RG to the extent that it is applicable to the similar requirements of 10 CFR 73.51.

Applicable Rules and Regulations

- 10 CFR Part 73, Section 73.1, "Purpose and scope," requires that licensees establish and maintain a physical protection system which 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 Part 73, Section 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," requires that each nuclear power reactor licensee or applicant under 10 CFR part 50 or 52 shall implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan.

- 10 CFR Part 73, Section 73.56, "Personnel access authorization requirements for nuclear power plants," requires that the licensee shall establish, implement and maintain an access authorization program and implement the requirements of this section through its Commission-approved Physical Security Plan.

- 10 CFR Part 73, Section 73.58, "Safety/security interface requirements for nuclear power reactors," requires that the licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

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

and qualification plan to ensure that those individuals who are assigned to perform duties and responsibilities required for the implementation of the Commission-approved security plans, licensee response strategy, and implementing procedures are properly suited, trained, equipped, and qualified to perform their assigned duties and responsibilities.

- 10 CFR Part 73, Appendix C, "Licensee Safeguards Contingency Plans," describes requirements for a documented plan to give guidance to licensee personnel in order to accomplish specific defined objectives in the event of threats, thefts, or radiological sabotage relating to nuclear power reactors.

Related Guidance

- RG 1.206, "Combined License Applications for Nuclear Power Plants" (Ref. 5), describes guidance regarding the information to be submitted in a COL application for a nuclear power plant.

- RG 5.12, "General Use of Locks in Protection and Control of Facilities and Special Nuclear Materials" (Ref. 6), provides criteria that the NRC staff considers acceptable for the selection and use of commercially available locks in the protection of facilities and special nuclear material.

- RG 5.44, "Perimeter Intrusion Alarm Systems" (Ref. 7), describes the functions of perimeter intrusion detection sensors and detection methods and systems testing that the NRC staff considers acceptable for meeting provisions contained in the requirements of 10 CFR 73.55(i) and 10 CFR 73.55(n).

- RG 5.66, "Access Authorization Program for Nuclear Power Plants" (Ref. 8), describes methods and processes that the NRC staff considers acceptable for meeting the requirements of 10 CFR 73.56 and 10 CFR 73.57.

- RG 5.68, "Protection Against Malevolent Use of Land Vehicles at Nuclear Power Plants" (Ref. 9), provides an approach that the NRC staff considers acceptable for meeting the requirements of 10 CFR Part 73 related to protection against land vehicles used to transport personnel and/or their hand-carried equipment. In addition, this guide describes adequate protection measures that the NRC staff considers acceptable for addressing protection requirements associated with a land vehicle bomb assault.

- RG 5.69, "Guidance for the Application of the Radiological Design Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements" (Ref. 10), provides an approach that the NRC staff considers acceptable for applying the radiological sabotage design basis threat (DBT) in the design, development, and implementation of a physical protection program to satisfy the general performance objectives and requirements in 10 CFR 73.55. Note that RG 5.69 contains Safeguards Information (SGI) and is therefore not publicly available.

- RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 11), describes methods and processes that the NRC staff considersacceptable for meeting the requirements of 10 CFR 73.54.

- RG 5.74, "Managing the Safety/Security Interface" (Ref. 12), provides methods and processes that the NRC staff considers acceptable for managing the interface between plant operations functions and security functions and meeting the requirements of 10 CFR 73.58.

- RG 5.75 “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities” (Ref. 13) describes methods and processes that the NRC staff considers acceptable to meet the requirements of 10 CFR Part 73, Appendix B, Section VI.

- RG 5.76, “Physical Protection Programs at Nuclear Power Reactors” (Ref. 14), describes methods and processes that the NRC staff considers acceptable for generally meeting the requirements of 10 CFR 73.55. Note that RG 5.76 contains Safeguards Information (SGI) and is therefore not publicly available.

- RG 5.77, “Insider Mitigation Program” (Ref. 15), describes methods and processes that the NRC staff considers acceptable for implementing an effective Insider Mitigation Program required in 10 CFR 73.55(b)(9).

- NUREG-0800, Sections 13.6.1, “Physical Security - Combined License and Operating Reactors,” and 13.6, “Physical Security - Design Certification” (Ref. 16), describes a comprehensive physical security program for COL applicants and operating reactor licensees.

- RG 5.81, “Target Set Identification and Development for Nuclear Power Reactors” (Ref. 17), describes methods that the NRC staff considers acceptable for meeting the requirements of 10 CFR 73.55(f) for applicant or licensee analysis, development documentation, and reevaluation of target set elements and target sets, including preventive operator actions that may be credited to prevent core damage (e.g., non-localized fuel melting and/or core destruction) or spent fuel coolant and exposure of spent fuel. Note that RG 5.81 is designated as Official Use Only – Security-Related Information and is therefore not publicly available.

Purpose of Regulatory Guides

The NRC issues RGs to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency’s regulations, to explain techniques that the staff uses in evaluating specific problems or postulated events, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides guidance for implementing the mandatory information collections in 10 CFR Parts 50, 52 and 73 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), under control numbers 3150-0011, 3150-0151, and 3150-0002. Send comments regarding this information collection to the Information Services Branch, 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, 3150-0151, 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 request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

Table of Contents

B. DISCUSSION

Reason for Revision

This revision of the guide (Revision 2) renames the guide and consolidates, enhances, and clarifies previous staff guidance for the development of licensee site-specific physical security plans found in NUREG-0908, "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans" (Ref. 18), training and qualification plans as described in Section VI of Appendix B to 10 CFR Part 73, and safeguards contingency plans as described in Section II of Appendix C to 10 CFR Part 73. This revision to the regulatory guide includes clarifications provided by the staff in responses to Security Frequently Asked Questions (SFAQs) issued after Revision 1 was published, and contains a wide variety of editorial changes to the overall Revision 1 content. In addition, because of the similarities between physical protection programs at general license ISFSIs and specific license ISFSIs, this revision of RG 5.54 provides licensees with guidance for developing physical security plans, training and qualification plans, and safeguards contingency plans that may be considered for use by specific license ISFSI licensees, as appropriate, to meet the requirements of 10 CFR 72.180. Lastly, this revision aligns this regulatory guide with revisions to RG 1.206, and NUREG-0800, Sections 13.6.1, "Physical Security - Combined License and Operating Reactors," and 13.6, "Physical Security - Design Certification."

Background

This RG applies to licensees with and applicants for a nuclear power reactor operating license that are required to have a physical security plan and a training and qualification plan as described in 10 CFR 50.34(c)(2); and a safeguards contingency plan as described in 10 CFR 50.34(d)(2). This guide also applies to licensees and applicants for a nuclear power reactor combined license that are required to have a physical security plan as described in 10 CFR 52.79(a)(35)(i), a safeguards contingency plan as described in 10 CFR 52.79(a)(36)(i), and a training and qualification plan as described in 10 CFR 52.79(a)(36)(ii); and supplements guidance contained in RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR) Edition)." In addition, the guidance may be used to further inform, but does not substitute for, the guidance found in RG 3.50, "Standard Format and Content for a Specific License Application To Store Spent Fuel and High-Level Radioactive Waste," for 10 CFR Part 72 licensees in meeting the requirements of 10 CFR 73.51, 10 CFR 72.24(o), and Part 72, Subpart H.

Licensee security plans describe how the licensee implements, and meets the specific requirements applicable to, its physical protection program. Commission requirements that are pertinent to the format and content of the required security plans for power reactor licensees are addressed in 10 CFR 73.55(a) through (c). These Commission requirements address general performance criteria and standards that would be met through the effective implementation of the Commission requirements addressed in 10 CFR 73.55(d) through (r) and Appendices B and C to 10 CFR Part 73.

The NRC staff's review of the licensee security plans includes the design of engineered physical security systems, hardware, and features; administrative controls; management systems; and organization. The scope of the NRC staff review is outlined in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," and includes all information and descriptions that the NRC staff will employ to verify and document the licensing bases for a site-specific physical protection program. The NRC staff review includes, but is not limited to, the design, construction, and installation of physical security equipment and systems; the establishment of a management system that contains a clear and understandable chain of command that includes position titles and duty descriptions; the development of a training and qualification program that ensures all

individuals assigned security duties are trained, qualified, and equipped to effectively perform assigned duties and responsibilities; the development of predetermined response plans for contingency events; the development of a maintenance system to ensure that all security-related equipment is in sufficient supply and is capable of performing its intended function when needed; as well as the development of site-specific security measures, policies, and procedures needed to implement the physical protection program.

These programmatic elements of the physical protection program, as described in the security plans, provide the technical basis to support a conclusion that the physical protection program will 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. Therefore, it is important that the licensee's descriptions in the security plans of how it will implement the requirements in 10 CFR 73.55(d) through (r) and Appendices B and C to 10 CFR Part 73 contain sufficient detail.

The technical basis for the NRC's approval of each security plan is described in the section titled "Limitations on NRC Approval" within each NRC staff developed Safety Evaluation Report (SER). This SER section can be summarized as follows:

> In general, the NRC's review and approval of each licensee's security plans is focused on ensuring that the necessary programmatic elements are contained in these plans to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The NRC has determined that if effectively implemented these plans will provide the required high assurance. The burden to effectively implement these plans remains with the licensee. Effective implementation is dependent on the procedures and practices the licensee develops to satisfy the programmatic elements of its security plans. *As such, the NRC's approval of the licensee's security plans is limited to the programmatic elements necessary to provide the required high assurance. Should deficiencies be identified with the programmatic elements addressed in these plans, the plans shall be corrected to address the deficiencies.*

Given the site-specific conditions that exist at each licensee facility, the security plans must be of sufficient detail for the reader to understand and determine how the plan satisfies all the requirements in 10 CFR Part 73. Although a licensee's physical protection program must comply with the Commission requirements contained in 10 CFR Part 73, it is not necessary for the licensee to explicitly repeat each of these Commission requirements, individually, in the site-specific security plans. However, the licensee's security plans must comprehensively describe how all Commission requirements will be accounted for and implemented by the physical protection program.

Comprehensive security plans should describe, in sufficient detail, all programmatic elements utilized or relied upon by the licensee to perform the functions required to implement the physical protection program in accordance with Commission requirements. The security plans should include detailed information that provides an understanding of how compliance with each requirement supports, or is supported by, other programmatic elements and components of the physical protection program. The specific programmatic elements described and the level of detail needed in each description is determined by each licensee based upon the design of each physical protection program and the site-specific conditions that must be accounted for in the design. For example, an acceptable physical security plan should contain a description of how the physical protection program is designed to prevent significant core damage and spent fuel sabotage. The underlying basis for how this requirement is met must be established through the licensee's description of the design, implementation, and use of security

equipment, systems, and processes that are relied upon to ensure that the capabilities to detect, assess, interdict, and neutralize threats are maintained at all times. To adequately describe the use of security equipment, systems, and processes, the licensee should describe the underlying basis for the design and intended function of components, equipment, systems, or processes to include any site-specific conditions that provide the technical reason or rationale for the stated function that is performed. For the purpose of determining the appropriate level of detail to be contained in a security plan description, the licensee should consider how the component, equipment, system, or process being described is integrated into the overall physical protection program; which Commission requirements apply to that component, equipment, system or process in addition to what site-specific conditions necessitate the measure and impact the description; and how that component, equipment, system, or process supports or provides a basis for a high assurance determination by the NRC.

The Commission's requirements in 10 CFR 73.55(a) state that the security plans must identify, describe, and account for site-specific conditions that affect the licensee's capability to satisfy the requirements of 10 CFR 73.55. This requirement is important because in some cases, it is the site-specific condition that provides the information needed to understand why a licensee is implementing a specific security measure in the manner that is described in the security plan. A simple statement describing compliance with a given Commission requirement does not provide sufficient information to the reader to determine how the licensee is meeting that requirement. The underlying purpose of a licensee security plan is to describe specifically how Commission requirements are being met at the site to which the security plan applies. For example, where a licensee's facility has equipment or systems that have been determined to be important to safety, but have not been determined to be "vital," and the equipment or systems are not being protected as vital or contained within a vital area, the licensee should consider the need to describe this condition in the security plan as well as the technical basis for the determination. The discussion of the technical basis that supports a site-specific determination should include any information that demonstrates an NRC position regarding the licensee's determination and when the issue was last analyzed. The technical basis for any such determinations that were addressed prior to September 11, 2001, or prior to the 2009 revised Part 73 rulemaking, and are not currently addressed in the security plans, should be reconsidered for consistency with current physical protection needs and included in future revisions to the security plans. It is the intent of this RG to provide pertinent information that would assist a licensee in determining when and how this site-specific information should be addressed and provided in a security plan.

The Commission's requirements contained in 10 CFR 73.55(b) state that each licensee shall establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. A licensee achieves this objective through the effective and integrated implementation of all programmatic elements and components that make up the physical protection program. A determination that the high assurance objective has been met by a licensee is achieved through a review of the compilation of the information (comprehensive descriptions) contained in the licensee's security plans; the conduct of NRC inspections; and vigilance on the part of the licensee to identify and correct problems that impact the effectiveness of the physical protection program, including changes to site-specific conditions.

The Commission's requirements contained in 10 CFR 73.55(c) generally address the required content of the licensee security plans. The security plans must describe how the licensee will implement Commission requirements and must describe site-specific conditions that affect how the licensee implements Commission requirements. Specifically, 10 CFR 73.55(c) states that the licensee shall establish, maintain, and implement a Physical Security Plan which describes how the performance objective and requirements of 10 CFR 73.55 will be implemented; a Training and Qualification Plan that

describes how the criteria set forth in 10 CFR Part 73, Appendix B will be implemented; a Safeguards Contingency Plan that describes how the criteria set forth in 10 CFR Part 73, Appendix C will be implemented, and a Cyber Security Plan that describes how the criteria in 10 CFR 73.54 will be implemented.[1] The requirements further state that implementing procedures must document the structure of the security organization and detail the types of duties, responsibilities, actions, and decisions to be performed or made by each position of the security organization.

Security plans likely contain Safeguards Information (SGI). As described in 10 CFR 73.55(c)(2), licensees shall protect security plans and other security-related information against unauthorized disclosure in accordance with the requirements found in 10 CFR 73.21. Therefore, licensees must ensure that all licensee security plan submissions and amendments thereto are protected accordingly.

Harmonization with 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 develops safety standards for protecting people and the environment from harmful effects of ionizing radiation. These standards provide a system of safety fundamentals, requirements, and guides reflecting an international consensus on what constitutes a high level of safety. Pertinent to this regulatory guide, IAEA Nuclear Security Series No.13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)" (Ref. 20), provides a framework to develop or enhance a physical protection program. This RG is generally consistent with the principles in IAEA INFCIRC/225/Revision 5).

[1] This guide does not contain NRC staff guidance for the development of the Cyber Security Plan. That guidance can be found in RG 5.71.

C. STAFF REGULATORY GUIDANCE

Consistent with 10 CFR 50.34(c); 50.34(d); 52.79(a)(35); and 52.79(a)(36), each application for an operating license or combined license subject to the provisions of 10 CFR 73.55 must include a Physical Security Plan, a Training and Qualification Plan, a Cyber Security Plan, and a Safeguards Contingency Plan. These four plans describe the licensee's physical protection program that will be used to prevent radiological sabotage in accordance with Commission requirements.

10 CFR 73.55(a) states in part that each nuclear power reactor licensee shall implement the requirements of 10 CFR 73.55 through its Commission approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan, referred to collectively as ‘‘security plans,” and that the security plans must identify, describe, and account for site-specific conditions that affect the licensee’s capability to satisfy the requirements of 10 CFR 73.55.

Applicants and licensees should frame the presentation of information in their security plans plans as structured in this regulatory guide. Providing the NRC staff with a document that conforms to this regulatory guide in format and content will assist the NRC staff in its review and may expedite the review process. Licensees may also apply the presentation format as constructed in the NRC staff endorsed Nuclear Energy Institute (NEI) document NEI 03-12, “Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]” (Ref. 19). When a licensee relies on the presentation format of NEI-03-12, the licensee should ensure that the content guidance contained in this regulatory guide has been adequately reviewed and evaluated. Each licensee should evaluate and confirm that the generic text used in NEI-03-12 is applicable to its facility as written, and where prompted within the NEI 03-12 template, the insertion of site-specific information should follow the content guidance provided herein. For example, where the generic language contained in the NEI 03-12 is not applicable to a licensee’s site-specific condition(s) or does not adequately describe site-specific conditions, the licensee is responsible for providing appropriate site-specific details and descriptions within the plans to adequately describe the site-specific conditions, and how the associated regulatory requirement is satisfied by the licensee’s physical protection program, to include how implementing procedures ensure that required functions are performed effectively. Licensees are responsible for ensuring that the nature of the condition is clearly described, including the manner in which the licensee’s implementation of the plans will satisfy regulatory requirements.

1. Physical Security Plan

As described in 10 CFR 73.55(c)(3), the licensee shall establish, maintain, and implement a Physical Security Plan which describes how the performance objective and requirements set forth in 10 CFR 73.55 will be implemented.

1.1 Security Organization

As described in 10 CFR 73.55(d)(1), the licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of 10 CFR 73.55. As further required in 10 CFR 73.55(d)(2), the security organization must include: (1) a management system that provides oversight of the onsite physical protection program, and (2) that at least one member is onsite and available at all times, has the authority to direct the activities of the security organization, and is assigned no other duties that would interfere with this individual’s ability to perform these duties in accordance with the security plans and the licensee protective strategy.

The physical security plan should describe and/or confirm the following:

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

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

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

e) The structure and hierarchy of the management system that provides oversight of the onsite physical protection program. The physical security plan should provide an organization chart/diagram displaying relevant positions/titles in a command-and-control structure; describe the member of the security organization by position title and duty description, who will be available at all times to respond to a security event and direct the activities of the physical protection program; and confirm that there will be no duty assigned to this member that would interfere with their ability to direct physical protection program functions and activities. The management structure description should include the chain of command that will be used in the event that the primary individual is incapacitated or otherwise unable to perform these duties. The physical security plan should clearly establish the hierarchical separation and functional integration between the security organization and operational organizations.

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

g) The licensee has developed and implemented training and qualification standards and requirements for non-security licensee or contract employees who are assigned to perform any duty or activity that is required for or supports the licensee's implementation of the physical protection program. The physical security plan should confirm that no person will be permitted to perform any security program duties or activities until that person has demonstrated the requisite knowledge, skills, and abilities (including physical attributes such as sight and hearing) necessary to successfully perform that duty or activity, as described in the licensee's Commission-approved training and qualification plan.

1.2 Physical Barriers

As described in 10 CFR 73.55(e), "Physical barriers," each licensee shall identify and analyze site-specific conditions to determine the specific use, type, function, and placement of physical barriers needed to satisfy the physical protection program design requirements of 10 CFR 73.55(b).

a) The physical security plan should contain a description of the function to be performed by each type of barrier/barrier system used at the site, including placement and construction standards, and should describe in sufficient detail how each barrier/barrier system will provide the intended function for deterrence, delay, or support of the licensee's access control functions. Additionally, the physical security plan should describe how openings in any barrier, to include underground pathways and/or unattended openings, are secured and monitored to prevent exploitation. Applicants and licensees may find NUREG/CR-6190, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants: Vehicle Barrier System Selection Guidance" (Ref. 21), useful in designing and siting vehicle barrier systems to provide adequate protection from detonation of land vehicle bombs. For additional information on barrier design and engineering, licensees may consult the references found in Appendix A of RG 5.69, "Guidance for the Application of the Radiological Design Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements."

As described in 10 CFR 73.55(e)(5) and 73.55(i)(4)(iii), the licensee must ensure that the reactor control room, the central alarm station (CAS), the secondary alarm station (SAS) (for new reactors licensed after May 26, 2009, the effective date of the 2009 Part 73 rulemaking), and the location within which the last access-control function for access to the protected area is performed are bullet-resisting.

b) The physical security plan, at a minimum, includes complete descriptions of the structures described in the above paragraph10 CFR 73.55(e)(5) and 10 CFR 73.55(i)(4)(iii), and describes how the licensee ensures that the structures are "bullet-resisting" (sometimes referred to as "bullet resistant"). The physical security plan should describe how the structures provide protection against complete penetration, passage of fragments of projectiles, and spalling (fragmentation) of the protective material that could cause injury to a person standing directly behind the bullet-resisting barrier. The physical security plan should confirm that the above structures have a minimum capability of resisting a high-powered rifle round, as discussed in RG 5.76 "Physical Protection Programs at Nuclear Power Reactors."

As described in 10 CFR 73.55(e)(6), the licensee shall establish and maintain physical barriers in the owner controlled area (OCA) as needed to satisfy the physical protection requirements of Section 73.55(b).

c) Licensees are permitted to utilize natural barriers as a component of the physical barrier system where such natural barriers contain the requisite physical features, such as sufficient size and strength, that would satisfy the physical protection design requirements of 10 CFR 73.55(b). However, where natural barriers do not meet design characteristics and performance standards necessary for implementing the licensee's protective strategy, licensee analysis and installation of physical barriers would be required. The physical security plan describes the barriers used (natural or man-made), the function to be performed, and the features or construction standards that provide the bases for determining that the barrier can and will perform its function.

d) The physical security plan should describe the manner in which the licensee's unique natural terrain features meet the objective of this section and further, describes the design and construction characteristics of any installed physical barrier and how the combination of these barriers support the licensee's protective strategy. Applicants and licensees may find U.S. Army Corps of Engineers Protective Design Center Technical Report (PDC TR) 06-05, Rev.1, "Evaluating Adequacy of Landform Obstacles as Vehicle Barriers" (Ref. 22), helpful, as well as additional guidance in RG 5.76 (see Ref. 14). Applicants and licensees may also find NUREG/CR-4250,[2] "Vehicle Barriers: Emphasis on Natural Features" (Ref. 23), helpful in assessing natural terrain intended for use in their vehicle barrier configuration.

As described in 10 CFR 73.55(e)(7), the licensee must maintain an isolation zone in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone must be of sufficient size to permit observation and assessment on either side of the protected area barrier, monitored with intrusion detection equipment designed to satisfy the requirements of 10 CFR 73.55(i), capable of detecting actual or attempted penetrations of the protected area before the act can be completed, and monitored with assessment equipment designed for real time and video playback of images. Any obstructions that would prevent the licensee's performance of required observation and assessment functions must be located outside of the isolation zone.

e) Each licensee is responsible for determining the isolation zone size and dimensions that meet the site-specific needs of its facility. Consistent with 10 CFR 73.55(b)(4), the specific size and dimensions of an isolation zone at any one NRC-licensed facility must account for site-specific conditions such as facility layout and geography in its design and should be documented in a site-specific analysis. For example, a professionally accepted generic standard for this type of an area is described in the United States Army Field Manual, FM 3-19.30 "Physical Security" (Ref. 24), which states in part that "A clear zone of 20 feet or greater should exist between the perimeter barrier and exterior structures, parking areas, and natural or cultural features."

f) The physical security plan should describe the depth or width of the isolation zone on the exterior of the protected area barrier, as well as on the interior of the protected area barrier. In addition, the physical security plan should describe the manner in which intrusion detection equipment provides monitoring and assessment of the isolation zone and how the intrusion detection system is designed and configured in order to provide for

[2] The NRC staff has identified errors in Sections 2.7 and 2.8 of NUREG/CR-4250. As such, when a licensee, applicant, or certificate holder desires to perform hang-up or nose-in failure calculations found in Sections 2.7 and 2.8 of NUREG/CR-4250, corrected guidance found in PDC-TR 06-05 should be utilized. The remainder of NUREG/CR-4250 is correct and may be utilized.

video capture and play-back of attempted or actual intrusion, including how spurious or false alarm actuation is confirmed. Furthermore, the physical security plan should describe the manner in which the licensee prevents the isolation zone from becoming encumbered by obstructions that would prevent observation or assessment. The physical security plan should describe typical obstructions that may occur during outage or construction activities and describe how these temporary obstructions would be compensated to maintain detection, observation, and response.

As described in 10 CFR 73.55(e)(8), the licensee must ensure that the protected area perimeter is protected by physical barriers. The physical security plan should:

g) Describe how the licensee limits access into the protected area to only those personnel, vehicles, and materials required to perform official duties.

h) Describe the licensee's engineering design and approach to channel personnel, vehicles, and materials to identified designated locations, and/or access control portals.

i) Describe the licensee's engineering design and approach to ensure protected area barriers are separated from any other barrier designated as a vital area barrier, unless specifically identified and addressed in the plan.

j) Confirm that any fencing used to satisfy a Commission requirement for a physical barrier is constructed of at least equal to 11 AWG (American Wire Gauge) chain link, a top guard of at least three strands of barbed wire (or similar material) on brackets angled inward or outward between 30 and 45 degrees from vertical, with an overall fence height of 8 feet from ground surface, in accordance with the definition of "physical barrier" in 10 CFR 73.2. The physical security plan should describe the methodology and periodicity to be used by the licensee for identifying, correcting, and compensating for discovered degradation of physical barriers. Additionally, the physical security plan should describe the design and installation characteristics that the licensee employs to ensure that the fence fabric cannot be raised or lifted at or from the bottom, and should specify how areas susceptible to wash-out/erosion of ground surface will be monitored and repaired in a timely manner to prevent further compromise. Licensees should include whether the licensee uses barbed wire or similar material such as razor wire (i.e., barbed tape) as a supplement to or replacement for barbed wire.

k) Describe the design, substance, and configuration of controls that the licensee has established for ensuring that personnel, vehicles, and materials have limited access to the protected area, and that personnel, vehicles, and materials are controlled while within the protected area. The physical security plan should include a detailed description of protected area barriers that is consistent with the definition of physical barrier provided in 10 CFR 73.2, and how the licensee ensures that penetrations of the protected area barrier, such as unattended openings that intersect a security boundary (e.g., underground pathways), are protected. The physical security plan should describe how unattended openings and underground pathways are protected (as required by 10 CFR 73.55(i)(5)(iii)), and confirms that any unattended opening of a size/dimension and environment that could be exploited as a pathway will be secured upon discovery or compensated until properly secured. Specific guidance regarding unattended openings can be found in RG 5.76. Additional information regarding a commonly accepted professional standard can be found in the U.S. Army Field Manual 19-30, which specifies that any opening equal to or greater than 96 square inches, (with at least one dimension

being equal to or greater than 6 inches) should be protected by physical barriers and monitored to detect exploitation.

l) Describe the manner in which emergency exits are secured but also allow for prompt access during emergencies. In addition, the licensee's security plan should describe the means for ensuring detection, assessment and interdiction where structures or buildings form portions of the protected area perimeter barrier, absent an isolation zone, and how these structure or building walls are provided with barriers or interferences that prevent them from being scalable without detection. The physical security plan should describe the configuration and construction of all access portals to include any portion of a protected area barrier that may be an interior wall, and any physical protection measures that are applied in areas that may be concealed from view (e.g., the area above a false ceiling inside the access portal). The physical security plan should describe the process implemented by the licensee to perform periodic checks of all exterior areas of the protected area, excluding hazardous areas.

As described in 10 CFR 73.55(e)(9), the licensee must ensure that vital equipment is located only within a vital area. The licensee must protect vital area access portals and emergency exits with intrusion detection equipment and locking devices.

m) The physical security plan should describe the types of intrusion detection systems, how the systems are monitored, and the types of locking devices used to include biometrics or key and lock controls.

n) The physical security plan should describe the design and designation of each vital area, consistent with the definition of vital equipment as described in 10 CFR 73.2, and describe how the licensee's site-specific analysis has included these structures as vital areas required by regulation. The physical security plan describes the licensee's implementation of access portal intrusion detection and monitoring at vital areas. The physical security plan should confirm that the secondary power-supply system for alarm-annunciation equipment and the secondary power-supply system for non-portable communication equipment are located within the vital areas.

As described in 10 CFR 73.55(e)(10), the licensee must establish and maintain vehicle control measures, as necessary, for land and waterborne vehicles.

o) The physical security plan should provide a description of the licensee's design and implementation of active and passive barriers (vehicle barrier systems) that protect against the effects of the design basis threat of radiological sabotage vehicle bomb assault, including the stand-off distances adequate to protect those personnel, equipment and systems necessary to prevent significant core damage and spent fuel sabotage.

p) The physical security plan should include a discussion of the process employed or implemented by the licensee to periodically evaluate the performance of barriers and surveillance systems, including a description of measures that the licensee will implement, to ensure that active barriers are placed in, or remain in the denial position during any loss of power to these systems. The physical security plan should describe the licensee process to periodically review the site-specific conditions and assumptions that were considered or made for the purpose of determining required stand-off distances, and validate the accuracy of these conditions and assumptions as a basis for the conclusions and descriptions contained in the security plans.

q) The physical security should plan describe the periodic surveillance measures that the licensee implements to ensure that the licensee maintains an awareness of the condition of barrier systems, and to ensure an absence of tampering or degradation, or ensure the initiation of a response if these conditions are discovered. Licensees may find PDC TR 06-03, "Vehicle Barrier Maintenance Guidance" (Ref. 25), helpful in developing an acceptable vehicle barrier system inspection and maintenance program.

r) The physical security plan should describe the measures that the licensee has implemented to prevent any unauthorized access by locomotives or other vehicles over any existing railway systems.

s) The physical security plan should include details of activities coordinated and implemented between the licensee and governmental agencies for the protection of potential waterway approaches to the licensee site.

t) The physical security plan should describe waterway conditions normally experienced at the site, to include the ebb and flow of tides or other predicable increases or decreases in water levels such as historical flooding conditions.

u) The physical security plan should describe how the licensee accounts for predictable variations in water levels and describes the safety considerations that are specific to each mode of operation at the facility

v) The physical security plan confirms navigability considering the DBT waterborne bomb characteristics and does not rely solely upon a designation that the waterway is not navigable for commercial shipping or other use by members of the public.

w) The physical security plan should describe the licensee process to periodically review the site-specific conditions and assumptions that were considered or made for the purpose of determining navigability of waterways, the required stand-off distances, and describes how the licensee validates the accuracy of these conditions and assumptions as a basis for the conclusions and descriptions contained in the security plans.

1.3 Target sets

As described in 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. A site-specific analysis should identify equipment that is required to remain operable to prevent significant core damage and spent fuel sabotage, in accordance with 10 CFR 73.55(b), during each mode of operation.

a) The physical security plan should describe the licensee's process or methodology used to determine and select the equipment, components, systems, and configurations as target set elements or target sets, including the process for conducting the site-specific analyses of the individual and collective equipment, components, systems, and configurations. The licensee may find RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors" useful in developing this documentation.

b) The physical security plan should describe the process used to consider the impact of cyber attacks during the target set development and identification process, including how the use of multiple site functional disciplines is integrated into the process.

c) The physical security plan should identify and document all target set elements or target set equipment that are outside of the licensee's protected or vital areas. The physical security plan should describe the manner in which target set elements or target set equipment are accounted for, protected, and integrated as part of the licensee's protective strategy.

d) The physical security plan should summarize the processes and procedures implemented by the licensee for oversight of the configuration control process applied to target set elements and target sets. The physical security plan should describe the licensee's methodologies and implementation of configuration controls to ensure that any configuration changes to operating equipment or components established as a part of a target set will be addressed in the form of associated changes to those processes and procedures necessary for the licensee to maintain its protective strategy. Licensees may find RG 5.74, "Managing the Safety/Security Interface," useful in developing these processes and procedures.

1.4 Access Controls

As described in 10 CFR 73.55(g)(1), the licensee shall control all personnel, vehicle, and material access points in accordance with the physical protection program design requirements of 73.55(b).

a) The physical security plan should articulate how the licensee implements its configuration of access control portals, to include:

(1) A description of each access control portal located in the OCA and at the protected area perimeter, that includes the design and location of the access control portal, as well as the type of access control portal, (e.g., vehicle or personnel) and whether the access control portal is a vestibule outside of, or is contiguous with, the barrier through which access is controlled.
(2) A description of how each access control portal is equipped, the locking devices that are present, the available intrusion detection and surveillance equipment, and the licensee's compensatory measures when the licensee disables the intrusion detection and surveillance equipment or locking devices locally at the equipment installation point.
(3) A description of any overhead ceiling areas that could conceal unauthorized activities adjacent to the PA perimeter or an interior wall that forms a portion of the protected area barrier.
(4) A description of how the licensee provides supervision and control of the badging process. A security plan should describe how the licensee prevents intended or unintended bypass of access control equipment that is located outside of the licensee's protected area boundary.
(5) A description of the process and considerations that the licensee implements to limit unescorted access to protected and vital areas during non-emergency conditions to only those persons who are required to have unescorted access to the licensee's protected area, and to each vital area, necessary for the actual performance of an individuals assigned duties and responsibilities. Licensees may find 10 CFR 73.56(j), and RG 5.77, "Insider Mitigation Program," useful in

defining and applying the need for unescorted access and unescorted access authorization.

(6) A description of the processes and procedures used to assign an individual the responsibility of controlling admission to the protected area and how this person is isolated within a bullet-resisting structure that will ensure the individual's ability to respond to any threat condition and summon assistance, if required. Licensees should describe the manner in which it implements the last access control function when this function is routinely controlled by electronic means (e.g., biometrics) and continuously observed by an individual from within a bullet-resisting structure.

b) The physical security plan should describe how the licensee implements its design and configuration of vehicle barriers, including its control of vehicles while vehicles are inside the protected area, to include:

(1) A description of how the licensee physically controls vehicle barrier portals to ensure that only authorized vehicles are able to enter the OCA and/or protected area through the vehicle portal.

(2) A description of controls and procedure(s) that the licensee implements to conduct searches of vehicles and materials on or in vehicles for contraband or any other material or device that could be used to commit radiological sabotage or could be used to further any effort to commit radiological sabotage. Additional guidance on vehicle searches is in section 1.5, "Search Programs."

(3) A description of the controls and procedure(s) that the licensee has established to validate that the vehicle being searched is authorized for entry into the licensee's protected area and that the material on or in the vehicle is authorized for entry into the licensee's protected area.

(4) A description of the equipment, location, processes, and procedures that the licensee implements to monitor and observe searches conducted at vehicle barriers, and to respond to vehicle barrier search locations as necessary to implement the licensee's protective strategy.

c) The physical security plan should describe the controls, process and procedure(s) that the licensee implements to establish control over all vehicles inside the licensee's protected and vital areas. The physical security plan should describe how the licensee ensures that vehicles are used only for authorized purposes and operated by licensee employees who have been granted unescorted access, or non-licensee employees who are being escorted. Additional controls for vehicles inside of the licensee's protected and/or vital areas may include:

(1) Licensee controls to ensure that vehicles inside of the licensee's protected area are limited for use to plant functions;

(2) Licensee controls to ensure that keys are removed from the vehicle when the vehicle is not in operation;

(3) Licensee controls to ensure that vehicles are secured or disabled when not in use; and

(4) Licensee controls to ensure that vehicles that are transporting hazardous materials while inside of the licensee's protected area are always escorted by an armed member of the security organization.

d) The physical security plan should include a description of the processes, controls and procedures that the licensee implements before allowing personnel to gain unescorted or escorted access into the protected area and will describe the controls and processes for ensuring that the person requesting the access has or is not currently denied access to any other NRC licensed facility. Licensees may find RG 5.66, "Access Authorization Program for Nuclear Power Plants," useful in articulating their processes.

e) The physical security plan should describe how the licensee implements its vital area access control processes, to include:

(1) The controls, processes, and procedures employed by the licensee for the development and maintenance of one or more access control lists that contain descriptive and identifying information regarding all of the personnel who are currently granted unescorted access and to which vital areas these personnel have unescorted access.

(2) The controls, processes, and procedures employed by the licensee for responding to any site-specific credible threat or other credible threat information, including any credible insider threat. Procedures would typically include how and at what point the licensee implements its two-person (line-of-sight) process and how the licensee controls work assignments during both non-emergency and emergency conditions, for all personnel assigned duties requiring access to vital areas. This description should specify the access controls used to ensure that no one individual can be granted unescorted access to vital areas upon implementation of the two-person (line-of-sight) process under both non-emergency and emergency conditions.

(3) How the licensee's two-person (line-of-sight) process ensures coordination with all other site plans and procedures to avoid conflict, as required by 10 CFR 73.55(b)(11) and to ensure effective implementation when needed. To accomplish this, the physical security plan should account for the staffing levels necessary to implement each of the licensee's site plans and procedures for both normal and emergency conditions. The description of the two-person (line-of-sight) process should identify the personnel required to staff and implement each plan and procedure, whether sufficient staffing is onsite or must be re-called to meet the staffing needs of each plan and procedure, including, but not limited to, the site protective strategy, fire protection plan, emergency plan, and emergency plan for 10 CFR 50.54(hh) (aircraft threat).

f) The physical security plan should describe how the licensee implements its access control systems and procedures, including the two-person (line-of-sight) process, to ensure that authorized individuals are assured prompt access to the licensee's protected and vital areas during emergency conditions. The physical security plan should describe the licensee's approach for granting access to both onsite and offisite personnel during both planned and unplanned emergent conditions that could become emergency conditions and result in the need for a response from offsite resources. The physical security plan should describe the security procedures and processes that provide a sustained level of security presence and oversight, while at the same time, ensures that emergency personnel are provided prompt access to affected areas and equipment.

g) The physical security plan should describe how the licensee implements controls for the issuance, storage, annual audit, recovery, and retirement of keys, locks, combinations passwords and related access control devices, that would allow access to vital areas,

protected areas, security systems, and locked target set areas. Supplemental guidance for specific controls may be found in RG 5.71, "Cyber Security Programs for Nuclear Facilities," and RG 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials."

h) The physical security plan should describe how the licensee implements its photo identification badge issuance process for employees and non-employees, and should describe the key card controls and recordkeeping methodologies that the licensee implements to ensure:

(1) these devices (i.e., badges, key cards) are issued only to personnel that require access in the performance of official duties,
(2) real-time tracking/recordkeeping of vital and protected area access by individuals,
(3) recovery when employees and non-employees no longer require access or are terminated under both favorable or unfavorable circumstances,
(4) validation/verification of the badge or card holder's identification prior to re-entry after they have been removed from the protected area, and
(5) detection and response to any attempt by unauthorized personnel to bypass established photo identification badge issuance processes or key card controls, or otherwise obtain access control devices that would allow unauthorized access.

i) The physical security plan should describe how the licensee implements access controls for processing and escorting and controlling visitors, both as individuals and as groups, including the maximum number of persons to be escorted in vital areas and protected areas. The physical security plan should describe how the licensee verifies the identity of the visitor who will be escorted, confirms that the person who is assigned escort duties is authorized unescorted access to the areas in which he/she will be performing escort duties, and describes the licensee process to be used for documenting the assignment of escort duties. The physical security plan should also describe the process to be used for issuing a visitor badge and the instructions to be provided to each visitor to ensure issued visitor badges will be clearly displayed, such as attached to the visitor's upper torso in a manner that will clearly distinguish the person as a visitor, while the visitor is in the licensee's protected and vital areas.

j) The physical security plan should describe how the licensee implements its visitor control register to ensure that the register contains, at a minimum, the information required in 10 CFR 73.55(g)(7)(i)(C). The physical security plan should describe the manner in which the licensee ensures that persons requesting escorted access are not in a denied access status at any other licensee facility.

k) The physical security plan should describe how the licensee implements its program for training, qualifying and equipping (as appropriate) individuals who will be assigned personnel escort functions. Typically, non-security plant staff personnel may receive training to meet security escort requirements in accordance with the licensee's general employee training program and are assigned escort duties for visitors requesting access for business purposes or expected technical experts for professional meetings or consulting purposes. The physical security plan should describe how individuals providing the escort function for all other plant operational and maintenance activities are trained, qualified, and equipped in accordance with Appendix B to Part 73. In all cases, the physical security plan should describe how the licensee will ensure the following:

(1) the escort is authorized unescorted access to the area(s) where escort duties will be performed,
(2) the escort is provided a readily available means to summon assistance,
(3) when escorting a vehicle, the escort is provided a readily available means of continuous communication with the licensee's CAS or SAS, and
(4) the escort is generally knowledgeable of the work to be performed by the visitor in order to discern abnormal behavior or unauthorized activities.

1.5 Search Programs

As described in 10 CFR 73.55(h), the objective of the search program is to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage. To accomplish this, the licensee shall search individuals, vehicles, and materials consistent with the physical protection program design requirements in 10 CFR 73.55(b) and the function to be performed at each access control point or portal before granting access.

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

(1) A discussion of the implementing methodology and programmatic elements that are relied upon to ensure that the search functions are performed effectively, which may include a general discussion of how procedures will address the chosen methodology and programmatic elements. The physical security plan should discuss how the search processes ensure that all personnel, packages, and compartmented areas of a vehicle are searched; discuss how the search processes ensure that all prohibited items are detected; and clearly define and identify the items to be prevented from entering the OCA and potentially challenging the licensee protected area or target set components.
(2) A discussion of the implementing methodology and programmatic elements that are relied upon to ensure that the OCA vehicle search is conducted using equipment capable of detecting firearms, explosives, or other incendiary devices, or is conducted directly by personnel who apply visual and physical search functions, or by a combination of detection equipment and personnel actions. The discussion should confirm that the OCA vehicle search process is conducted by not less than two persons, one of which is armed and is an observer of the search being conducted. The function of the armed observer is to be able to take immediate defensive action(s) in the event of an observed condition for which a response is warranted, or an observed hostile or threatening action directed against the member of the security force conducting the search. Licensee procedures should describe the use of video surveillance equipment to observe the search and the role of a third person who can summon assistance if necessary.
(3) A discussion of the search functions performed by any Early Warning System established inside the OCA (personnel, materials, and/or packages). See section 1.6.f for further information regarding Early Warning Systems.

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

(1) A discussion of the manner in which the licensee subjects all persons (except federal, state and local law enforcement personnel on duty and on official business) packages and materials to a search through electronic means, as well as

visual or physical (hands-on) means, to ensure that all items within packages or luggage are identified as acceptable for entry into the licensee's protected area. The licensee may exempt from search all on duty armed security officers who have left the protected area and are, while still on-duty, re-entering the licensee's protected area.

(2) A description of the capabilities of the search equipment implemented to include the sensitivity settings established to ensure that the types of materials and composites that would be detected consistent with the requirements in the DBT.

(3) A discussion of the methodology and procedures applied by the licensee for conducting protected area searches when normal search equipment has been removed from service by the licensee for any reason, or when the equipment fails to operate as designed.

(4) A discussion of the process and procedures that the licensee implements when a licensee search discovers any firearm, explosive material(s), incendiary material(s), or any other material(s) that could be used to commit an act of radiological sabotage. At a minimum, the licensee must confirm that the individual and or vehicle will be denied access into the protected area until the licensee has determined that a threat no longer exists.

(5) A discussion of implementing procedures describing the methodology of the search process to be executed prior to a vehicle entering the protected area.

(6) A discussion of the specific materials that the licensee will except from search, including the basis for the exclusions and whether these exclusions are due to safety or operational considerations. The physical security plan should describe the licensee's implementing procedures for the specific security measures to be implemented for managing excepted materials. The physical security plan should describe how the licensee implements controls of locked storage areas or containers, how the licensee ensures that the materials within these locked storage areas or containers cannot be accessed until they reach their final destination, and how the licensee ensures that the locked storage areas or containers are opened only by persons familiar with the contents of the locked storage areas or containers.

(7) A discussion containing the description, procedures, and processes for the management of bulk materials. Licensees should be aware of the information contained in Security Advisory 06-04, "Implementing Search Requirements and Approved Exceptions for Packages and Materials at NRC Licensed Facilities" (Ref. 26), published September 6, 2006, as well as the decision tree chart found in SFAQ 10-03, "Verification of Bulk or Hazardous Materials" (Ref. 27), while developing these procedures and processes. The physical security plan should describe the licensee's implementation of processes that include confirmation that bulk materials are always escorted by an armed member of the licensee's security organization until the material reaches its final destination where the materials are removed from the delivery vehicle and verified by receipt inspection, and that this receipt inspection verification activity is not conducted adjacent to a vital area, unless offloading at that location is essential.

1.6 Detection and Assessment Systems

As described in 10 CFR 73.55(i)(1), the licensee shall establish and maintain intrusion detection and assessment systems that satisfy the design requirements of 10 CFR 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the licensee's protective strategy. An acceptable description of these systems in the physical security plan

includes all equipment that is relied upon by the licensee to provide intrusion detection and assessment of possible threats in the OCA, protected area, or vital area.

As described in 10 CFR 73.55(e)(6) "Owner controlled area," the licensee shall establish and maintain physical barriers in the OCA as needed to satisfy the physical protection program design requirements of 10 CFR 73.55(b). The phrase "as needed" allows licensees the flexibility to determine which, if any, site-specific physical protection program measures are appropriate within the OCA.

a) The physical security plan should describe the design of the licensee's intrusion detection system, and provides details describing how the licensee's intrusion detection systems are configured. Consistent with 10 CFR 73.55(i), the physical security plan must describe how, with each alarm annunciation, there is a concurrent video assessment of the annunciating alarm point that is displayed in not less than two continuously staffed onsite alarm stations.

b) The physical security plan should confirm that, for reactor facilities licensed prior to May 26, 2009 (the effective date of the 2009 Part 73 rulemaking), at least one alarm station is protected in accordance with the requirements of the CAS. For power reactors licensed after May 26, 2009, the physical security plan should confirm that both the CAS and the SAS are located, constructed, and equipped to the same standards and redundant capabilities.

c) The physical security plan should describe the licensee's implementation of its visual intrusion detection display of alarm points and its corresponding audio alarm announcement. In addition, the physical security plan should describe the follow-up operator assessment actions, including how the licensee ensures prompt and timely response to the location of the alarm, as well as the processes and procedures implemented for dispositioning alarms.

d) The physical security plan should describe the manner in which the IDS identifies the type and location of the alarm; how the IDS distinguishes among alarms related to a potential intrusion or the appearance of a tampering condition, and alarms that are the result of a system failure; and how the IDS indicates whether the system is operating on a back-up power supply in the event of a failure.

e) The physical security plan should describe how the licensee has ensured that the perimeter IDS remains on an uninterruptible power supply, and should specify the locations of the back-up power supplies.

f) Consistent with the flexibility provided by 10 CFR 73.55(e)(6), licensees may choose to implement physical protection measures, consisting of, but not limited to, physical barriers, intrusion detection systems, access portals, and search processes, inside the OCA that are in addition to, and are separate from, the isolation zone requirements in 10 CFR 73.55(e)(7) and protected area requirements in 10 CFR 73.55(e)(8). A licensee may choose to apply such measures in the OCA to provide additional delay; pre-screening of personnel, vehicles, and materials; and/or detection and assessment of unauthorized activities prior to gaining proximity to the protected area. Implementation of such measures is commonly refered to as an "Early Warning System." Where an Early Warning System is implemented to meet the requirements of 10 CFR 73.55(b), the Early Warning System is a required system. A required Early Warning System must meet all Commission requirements associated with the physical barriers, access portals, search

processes, and intrusion detection and must be described in the physical security plan. An Early Warning System will also be considered a required system where the licensee accounts for the system in developing pre-determined responder timelines. An Early Warning System that is not needed to meet Commission requirements is a voluntary enhancement that need not be discussed in the physical security plan, unless the licensee intends to seek regulatory credit for the additional margin of protection provided by the Early Warning System in support of a required programmatic element (for example, the additional margin for responder engagement time provided by early detection of an adversary). If the licensee intends to seek regulatory credit for the Early Warning System, then the licensee must describe the system in the Commission-approved security plans as a component of the physical protection program, and the system must be designed and maintained to effectively perform the intended function as described by the licensee in the physical security plan.. An acceptable physical security plan describes the design, functions, and capabilities of the system and describes how the system is integrated into the physical protection program. The description of the Early Warning System should focus on the "function" to be performed; the system design, to include location, components, structures, and equipment used to provide/accomplish the stated function; and how the system is integrated to augment and/or support all other physical protection program measures such as "initiating events." Early Warning Systems that are described in the physical security plan as a component of the physical security program must be included in the licensee's maintenance, testing, and calibration program; compensatory measures; and periodic reviews of the security program. For additional information refer to a letter from the NRC, dated May 26, 2016, titled "The U.S. Nuclear Regulatory Commission Inspection Approach Related to Industry Implementation of Early Warning Systems,"

As described in 10 CFR 73.55(i)(4), the licensee's two continuously staffed onsite alarm stations must be designed and equipped to ensure that a single act does not simultaneously disable both alarm stations and that the surviving alarm station, if one has been disabled, retains the ability to achieve its required functions.

g) The physical security plan should describe the measures that the licensee implements to ensure that the detection, assessment, and command and control functions will remain viable at all times including the manner in which the licensee ensures that these functions will be performed by trained and qualified personnel who are able to perform their alarm response functions without interference. The physical security plan should describe how the licensee implements predetermined and coordinated activities that ensure an adequate response to events, including the coordination of any response necessary from offsite resources.

h) The physical security plan should describe how the CAS (and, for reactors licensed after May 26, 2009, the SAS) is located inside of the licensee's protected area and describes how this alarm station is isolated in such a manner that it cannot be seen from the perimeter of the protected area. The physical security plan should describe and confirm how the personnel staffing the CAS and SAS will not be assigned any duties or otherwise encumbered in any manner that would interfere with their alarm response functions.

i) The physical security plan should describe and confirm how alarm station operators will not have the ability to unilaterally change alarm detection functionality and that alarm station operators in both the CAS and SAS are knowledgeable of and concur on the final disposition of each alarm.

As described in 10 CFR 73.55(i)(4)(iii), new power reactors licensed after May 26, 2009, must ensure that both the central and secondary alarm stations are constructed, located, protected, and equipped to the standards of the CAS.

j) The physical security plan should describe the design and implementation features that the licensee has established to ensure that each alarm station is equal and redundant and how the licensee ensures that all functions required to be performed in one alarm station, can be simultaneously performed in the alternate alarm station.

As described in 10 CFR 73.55(i)(5), the physical protection program must include surveillance, observation, and monitoring as needed to satisfy the design requirements of 10 CFR 73.55(b), identify indications of tampering, or otherwise implement the site protective strategy.

k) The physical security plan should describe how the licensee provides for the continuous observation and monitoring of the licensee's OCA, protected area, and vital areas. The physical security plan should describe how the licensee implements its normal and random patrol and inspection functions to ensure that, in addition to vital areas, target set elements are observed to ensure obvious indications of tampering are detected and that proper response to any such indication is initiated. The physical security plan should describe the design, construction, equipment, and function of any Early Warning Systems inside the OCA, if the licensee uses the Early Warning System to meet the requirements of 10 CFR 73.55(b) or intends to seek regulatory credit for the Early Warning System, as discussed in 1.6.f above. The physical security plan should describe the implementing procedures that are applied when any indication of tampering is suspected or investigated.

As described in 10 CFR 73.55(i)(6), the licensee shall ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy.

l) The physical security plan should describe how the licensee establishes and maintains the required illumination level of not less than 0.2 foot-candles, measured horizontally at ground level, in all isolation zones and appropriate exterior areas within the licensee's protected area. Where the licensee implements the use of low light technology to augment illumination levels necessary to implement the licensee's protective strategy, the physical security plan should describe the specific attributes of the augmentation, how the augmentation ensures the capability for observation by security force personnel, and the implementation decision points for these specific attributes.

1.7 Communication Requirements

As described in 10 CFR 73.55(j), licensees shall establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

a) The physical security plan should describethe types of communication technologies and capabilities provided within each of the licensee alarm stations and how these technologies are used to ensure communication with both onsite and offsite resources. The physical security plan should also describe the types of communication technologies and capabilities provided to security force personnel and contractor staff, including those personnel that may be used exclusively for escort functions, and how these technologies

are used to ensure that each of these personnel resources maintains continuous communications with each alarm station.

b) The physical security plan should describe how and the means through which the licensee's CAS and SAS maintain continuous communication capabilities between the licensee and local law enforcement authorities or other offsite resources, and with internal licensee management, including the licensee's operational control room.

c) The physical security plan should describe how the licensee maintains the operability of all of its non-portable communications equipment in the event of loss of normal power. The physical security plan should also distinguish those areas of the plant or site where communications equipment may not perform as designed, including areas in which portable communications equipment is known to work intermittently or not at all, and should specify the measures that the licensee implements to overcome the loss of routine communications capability.

1.8 Response Requirements

As described in 10 CFR 73.55(k), the licensee shall establish and maintain, at all times, properly trained, qualified, and equipped personnel to interdict and neutralize threats up to and including the DBT as defined in 10 CFR 73.1, to prevent significant core damage and spent fuel sabotage.

a) The physical security plan should describe the structure of the licensee's armed response team to include how this team is augmented by armed security officers within pre-determined timelines and/or how onsite response capabilities are strengthened by armed security officers to ensure that armed responders are able to carry out their duties and effectively implement the licensee's protective strategy.

b) The physical security plan must state the minimum number of armed responders necessary to satisfy the design requirements of 10 CFR 73.55(b) (i.e., prevent significant core damage and spent fuel sabotage) and implement the licensee's protective strategy. The physical security plan should specify and confirm that the number of armed responders identified in the security plans meets or exceeds this minimum number. The physical security plan should confirm that the specified minimum number of armed responders will be available at all times inside the protected area and will not be assigned duties that would interfere with their armed response team functions and/or their ability to execute the licensee's protective strategy.

c) The minimum number of armed responders may be augmented by armed security officers to carry out armed response duties within pre-determined timelines and ensure the effective implementation of the licensee's protective strategy. The physical security plan must document the number of armed security officers that are designated to strengthen onsite response capabilities and should confirm that these designated armed security officers are onsite and available at all times to carry out their assigned response duties. The physical security plan should confirm that armed security officers are not assigned duties that would interfere with their ability to augment armed responders within pre-determined timelines, or to strengthen onsite response capabilities consistent with the effective implementation of the licensee's protective strategy.

d) The physical security plan should describe how the armed response team is equipped in order to effectively implement the licensee's protective strategy. The physical security

plan should specify the types and number of firearms and ammunition that the licensee employs for implementing its protective strategy. Where the types of firearms and/or ammunition used by a licensee are prohibited by state law, the physical security plan will describe and confirm the authority under which the licensee is permitted to possess and/or use such firearms and/or ammunition. For example, if applicable, the physical security plan should confirm that the licensee has received Commission authority to possess and use such firearms and/or ammunition under Section 161A of the Atomic Energy Act of 1954, as amended (i.e., stand-alone preemption authority or combined preemption authority and enhanced weapons authority), or confirm that the state in which a site is located has, by state law or action by an authorized state representative, exempted the licensee from state firearms laws that would otherwise restrict the ability of licensee security personnel to possess and/or use such firearms and ammunition. The physical security plan should describe the sum of ammunition and related equipment that is readily available to armed responders and armed security officers, including the locations of ammunition and related equipment not in the possession of these armed personnel. The physical security plan should describe the integration of security-related operational requirements with technologies and how this integration is designed to interdict and neutralize adversaries, while at the same time ensuring the protection of responders.

e) The physical security plan should describe the performance sequences and conditions under which the licensee implements its graduated threat warning system by describing the licensee's protective measures and actions that will be implemented in the event of a heightened security threat, including the licensee's ability to reconstitute the licensee response force as necessary. The physical security plan should articulate how the licensee has ensured that the licensee's actions are consistent with the licensee's emergency plans.

1.9 Facilities Using Mixed-Oxide

As provided in 10 CFR 73.55(l)(3), licensees shall describe in the security plans the operational and administrative controls to be implemented for the receipt, inspection, movement, storage, and protection of un-irradiated mixed oxide (MOX) fuel assemblies.

a) The physical security plan should describe the processes that the licensee will implement for the receipt of MOX fuel assemblies and the planning and implementation activities that the licensee undertakes to apply tamper-indicating devices on fuel assemblies before the assemblies begin their transit to the licensee site.

b) The physical security plan should describe the licensee fuel assembly receipt staffing at the time of receipt, including security and operations associated disciplines. The physical security plan should describe and confirm the presence of at least one armed member of the security force, and that this member of the security force is not assigned an armed response function during the receipt and storage process.

c) The physical security plan should describe the processes that the licensee implements at the time of arrival at the licensee's site and before the licensee accepts custody of the fuel assemblies for verification of the integrity of the tamper-indicating devices that were installed on the MOX fuel assemblies prior to transit.

d) The physical security plan should describe the inspection process that the licensee implements to ensure that the MOX fuel assemblies have not been damaged during

transport, and describes the resolution measures that the licensee will implement should it discover any damage during the inspection.

e) The physical security plan should describe the inspection process that the licensee implements to ensure that the fuel assemblies do not have any unauthorized materials incorporated, in or on, shipping containers or transport vehicles, and describes the response or compensatory measures that the licensee will implement should it discover any such unauthorized materials.

f) The physical security plan should describe the processes that the licensee implements for moving MOX fuel assemblies from transport vehicles into position for storage, as well as processes for the relocation of MOX fuel assemblies for continued storage or relocation into the reactor.

g) The physical security plan should describe the integration of physical barriers with the existing water barrier that is the spent fuel pool. The description of the physical barrier configuration in the licensee security plan would typically describe and confirm that the MOX fuel assemblies are stored only within the spent fuel pool area and that there is a two barrier separation that does not include the water barrier provided by the confines of the spent fuel pool. The physical security plan should describe the licensee's implementation of its capability to detect, assess, interdict and neutralize any threat to MOX fuel assemblies, and describes the licensee's processes to maintain this capability.

h) The physical security plan should describe the material control and accountability processes that the licensee implements for the control and accountability of MOX fuel assemblies from receipt until final disposition.

i) The physical security plan should describe the measures that the licensee has implemented for routine disabling of any equipment used for the purpose of controlling the movement of MOX fuel assemblies that ensures that MOX fuel assemblies cannot be moved without preauthorization by authorized licensee management. The security plan should also articulate the person(s), by position within the licensee organization, who are authorized to permit MOX fuel assembly movement.

j) The physical security plan should describe the controls that the licensee has implemented that distinguish the establishment of a two-person line of sight control within the spent fuel pool at any time that MOX fuel assemblies must be relocated for any reason.

k) The physical security plan should describe the physical and operational controls that the licensee has established to prevent unauthorized use of equipment used for MOX fuel handling processes, as well as the processes and procedures that the license implements for the control of keys, locks and other access control devices that the licensee relies upon for restricting access to MOX fuel assembly storage areas. The operational controls contained within the security plan should include a description of the processes applied to ensure there is concurrent authorization from both the on-duty security shift supervisor, as well as the operations shift supervisor, prior to the movement of any MOX fuel assembly.

l) The physical security plan should describe the process that the licensee implements to ensure that armed security presence, specifically trained in MOX activities, has been established at any MOX fuel location prior to the removal of any access control devise,

during the transitioning of any MOX fuel assembly, and until all access control devices have been reinstalled, tested and determined operational.

m) The physical security plan should describe the process that the licensee implements to ensure that at least one armed security officer is present to maintain constant surveillance of any MOX assembly that has been removed from the spent fuel pool or the reactor.

1.10 Security Program Reviews

As described in 10 CFR 73.55(m), the licensee is required to conduct physical protection program reviews by individuals not involved in, or directly responsible for, managing or implementing the physical protection program. These reviews must be conducted not less than every twenty-four (24) months, or within twelve (12) months after initial implementation, or as necessary based on the licensee's site-specific analyses, assessments, or other performance indicators.

a) The physical security plan should describe the licensee's implementation of the processes and frequency it uses to perform a review and audit of the effectiveness of each element of the security program if used, and all processes that the licensee implements to address any findings from the results of each of these reviews and audits. The security plan should describe any formal review or audit conducted by personnel that are not within the security program reporting chain of command.

b) The physical security plan should describe the conditions and circumstances that would result in unplanned, unscheduled, or as-needed review of a single program element, multiple program elements, or the security program as a whole.

c) The physical security plan should describe the processes that the licensee uses for dispositioning any findings or recommendations that result from the review of the security program. The physical security plan should also describe the process for entering program reviews into the licensee's corrective action program including the structure that the licensee uses for reporting the implementation of actions taken from previous program reviews. The physical security plan should describe how the results of reviews and audits are presented to licensee management at least one level above onsite plant management.

1.11 Maintenance, Testing, and Calibration

As described in 10 CFR 73.55(n), the licensee shall establish, implement, and maintain a maintenance, testing, and calibration program to ensure that security systems and equipment , and secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended function.

a) The physical security plan should describe how the maintenance, testing, and calibration program is implemented at the licensee's site. The physical security plan should describe the conditional attributes of implementing actions associated with the maintenance, testing, and calibration program, how the licensee ensures that all deficiencies are tracked in the licensee's corrective action program, and how entries of the details of these deficiencies are appropriately protected from public disclosure. Licensees may place detailed technical requirements and operational considerations in implementing procedures.

b) The physical security plan should describe the processes that the licensee implements for ensuring that all IDS alarms are tested at least once every seven days when these systems have been in continuous use and prior to their return to service when they have been removed from service for preventive maintenance, repair, or troubleshooting. RG 5.44, "Perimeter Intrusion Alarm Systems," may assist licensees in developing testing protocols for some intrusion detection alarms.

c) The physical security plan should describe the process that the licensee implements to ensure that all communication equipment is operable at the beginning of each security work shift. The licensee may use any means at their disposal that will demonstrate and document that all communications equipment is operable and is functioning as designed.

d) The physical security plan should describe the testing protocols that the licensee implements to ensure that all search equipment is tested for operability not less that once each day, and tested for design performance at a frequency of not less that once every seven days.

e) The physical security plan should describe the protocols that the licensee implements to ensure that security-related devices or equipment located in hazardous areas are tested in a timely manner when the hazard no longer exists. The physical security plan should describe the licensee's application of "timely manner."

f) The physical security plan should describe the protocols and procedures that the licensee implements to ensure that all security equipment, in addition to IDS alarms described in 1.11.b above, are tested in accordance with these approved procedures prior to being placed in service when they have been removed from service for preventive maintenance, repair, or troubleshooting.

1.12 Compensatory Measures

As described in 10 CFR 73.55(o), the licensee shall identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components. The compensatory measures must be implemented within specific time frames necessary to meet the requirements in 10 CFR 73.55(b), and must be described in the security plans.

a) The physical security plan should describe the measures that the licensee implements whenever a security-related component has been removed from service or determined to be degraded in any manner, to achieve a level of protection that is equivalent to the level of protection provided when the equipment, system, or component was operable.

b) The physical security plan should describe the timelines within which compensatory measures will be implemented for degradation or inoperability of any security-related equipment, systems, or components.

1.13 Suspension of Security Measures

As described in 10 CFR 73.55(p), the licensee may suspend the licensee's implementation of security measures under emergency or severe weather conditions.

a) The physical security plan should describe the types of site-specific conditions under which the licensee will consider implementing the suspension of security measures in

accordance with 10 CFR 50.54(x) or 10 CFR 50.54(y), including the types of information that will be considered to confirm that no other action is immediately apparent to protect the public health and safety.

b) The physical security plan should confirm that any action that is undertaken to implement 10 CFR 50.54(x) or 10 CFR 50.54(y) is first approved by a licensed senior reactor operator and appropriately documented.

c) The physical security plan should describe the criteria for any licensee determination that weather is sufficiently severe to implement immediate actions to suspend security measures in order to protect the public health and safety.

d) The physical security plan should confirm that any action that is undertaken to suspend security measures due to severe weather conditions is first approved and documented by a licensed senior reactor operator, with input from the onsite senior security management.

1.14 Records

As described in 10 CFR 73.55(q), licensees are required to retain all records required to be kept by Commission regulations, orders, or license conditions.

a) The physical security plan should describe in detail all of the records that are maintained by the licensee. The physical security plan should describe the form (electronic or paper) of these records and confirm their complete, unfettered availability to Commission staff and inspection.

b) The physical security plan should confirm that the retention time for records is until the Commission terminates the license for which the records were developed, and that the licensee shall retain superseded portions of records for three years.

c) The physical security plan should confirm that written agreements with contracted resources that implement any portion of the licensee's security program are maintained for the duration of the contract. Written agreements should confirm that the contractor's records that were developed in association with fulfilling regulatory and security plan requirements are available to Commission staff as described in 10 CFR 73.55(q)(1).

d) The physical security plan should confirm that the licensee retains all reports of program reviews and audits for a period of three years after the review or audit was documented.

1.15 Alternative Measures

As described in 10 CFR 73.55(r), the licensee may provide an alternative physical protection measure different from one required by 10 CFR 73.55, if the measure meets the same performance objectives and requirements specified in 10 CFR 73.55(b) and the measure has been reviewed and approved by the Commission.

a) The physical security plan should uniquely identify and describe any site-specific condition or physical protection measure that is not consistent with Commission requirements and should confirm that the licensee has received the required approval from the Commission through appropriate licensing actions.

b) The physical security plan should uniquely identify the section of 10 CFR 73.55 that the alternative measure replaces, amends, or augments and should reference pertinent documentation addressing the licensee's request for Commission approval and the Commission's granting of the requested action, including any conditions, restrictions, or limitations assigned by the Commission to the approval.

c) The physical security plan should describe the measures taken to implement an alternative measure granted by the Commission, including how any conditions, restrictions, or limitations assigned by the Commission will be met.

2. Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties

As described in 10 CFR 73.55(c)(4), the licensee shall establish, maintain, implement, and follow a Training and Qualification Plan that describes how the criteria set forth in appendix B, section VI, to 10 CFR Part 73 will be implemented.

2.1 Introduction

As described in Section VI, paragraph A.1, of Appendix B to 10 CFR Part 73, the licensee shall ensure that the personnel who are assigned duties and responsibilities required to implement the Commission-approved security plans meet minimum training and qualification requirements to ensure each individual possesses the knowledge, skills, and abilities required to effectively perform assigned duties and responsibilities.

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

As described in Section VI, paragraph A.4, of Appendix B to 10 CFR Part 73, each individual assigned to perform security duties must demonstrate an ability to meet the requirements of the duties to be performed before they are assigned to perform those duties.

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

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

As described in Section VI, paragraph A.5 of Appendix B to 10 CFR Part 73, the licensee shall ensure that the training and qualification program simulates, as closely as practicable, the specific conditions under which the individual shall be required to perform assigned duties and responsibilities.

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

d) A training and qualification plan should describe the process applied to ensure that tasks performed to satisfy a training criteria/goal are performed commensurate with the conditions under which these task actions will be performed while implementing the licensee's security posture and protective strategy.

As described in Section VI, paragraph A.6 of Appendix B to 10 CFR Part 73, the licensee may not allow any individual to perform any security function, assume any security duties or responsibilities, or return to security duty until that individual satisfies the training and qualification requirements of the Commission-approved training and qualification plan.

e) A training and qualification plan should describe the procedures and process that the licensee implements to ensure that individuals have been fully qualified on tasks to be performed before they are assigned any security duties or responsibilities.

As described in Section VI., paragraph A.7 of Appendix B to 10 CFR Part 73, the licensee must maintain an annual training schedule at a nominal twelve (12) month periodicity. Annual requirements may be completed up to three (3) months before or three (3) months after the scheduled date. However, the next annual training must be scheduled twelve (12) months from the previously scheduled date rather than the date the training was actually completed.

f) A training and qualification plan should describe the procedures and processes that the licensee implements to ensure that training requalification schedules are maintained within the required nominal 12 month periodicity.

2.2 Employment Suitability and Qualification

As described throughout Section VI, paragraph B. of Appendix B to 10 CFR Part 73, individuals who are assigned security duties and responsibilities must meet minimum requirements to determine their initial and continued suitability (i.e., acceptability) and then must ensure that they are and continue to be qualified (i.e., proven capable) to provide the required services before fulfilling security-related assignments.

As described in Section VI, paragraph B.1.(a) of Appendix B to 10 CFR Part 73, individuals, must possess a high school diploma or pass an equivalent performance examination designed to measure basic mathematical, language, and reasoning skills, abilities, and knowledge required to perform security duties and responsibilities.

a) A training and qualification plan should describe the procedures and processes that the licensee implements to confirm that an individual possess a high school diploma.

b) Licensees may choose to accept a high school diploma from an accredited high school, or in the alternative, may administer or have administered, an equivalent performance examination designed to measure the attributes described above.

As described in Section VI, paragraph B.1.(a) of Appendix B to 10 CFR Part 73, an individual must have attained the age of 21 years if serving the licensee in an armed capacity, or must have attained the age of 18 if serving the licensee in an unarmed capacity.

c) A training and qualification plan should describe the documentation that the licensee will accept as a means to satisfy the above requirement. Licensees may use and apply the

same documentation requirements applied to meet the access authorization requirements in 10 CFR 73.56.

d) A training and qualification plan should describe how the licensee ensures that individuals who will be serving the licensee in an armed capacity meet suitability criteria for possessing firearms in accordance with applicable state laws and/or restrictions. Suitability may be determined, in part, through information that has been obtained during the completion of the individual's background investigation for unescorted access and/or Section 161A of the Atomic Energy Act of 1954, as amended, if applicable.

e) A training and qualification plan should describe the documentation that the licensee accepts to confirm that individuals are not prevented from possessing firearms as described in the applicable local, state, or federal firearms laws that would prohibit or restrict any individual from the possession or use of a firearm in the state in which the facility is located.

As described in Section VI, paragraph B.1.(b) of Appendix B to 10 CFR Part 73, the qualification of each individual to perform assigned duties and responsibilities must be documented by a qualified training instructor and attested to by a security supervisor.

f) A training and qualification plan should describe the documentation that the licensee employs to record the qualifications of each individual. A training and qualification plan should describe the processes used to ensure that instructors are certified or otherwise trained and qualified to provide the instruction for which they are responsible to document.

2.3 Physical Qualification

As described in Section VI, paragraph B.2 of Appendix B to 10 CFR Part 73, individuals whose duties and responsibilities are directly associated with the effective implementation of the Commission-approved security plans, licensee protective strategies, and implementing procedures may not have any physical conditions that would adversely affect their performance of assigned security duties and responsibilities.

a) A training and qualification plan should describe the physical requirements (e.g., ability to lift a specified poundage from the ground to waist level and from waist level to overhead; ability to traverse a specified distance in a specified time, including an ability to retain respiratory stability sufficient to engage a target at the conclusion of meeting a time and distance requirement) associated with meeting the performance attributes necessary for fulfilling security duties and responsibilities, including armed response duties and responsibilities.

b) Each licensee is responsible for developing and implementing a physical fitness program that is representative of the types of duties that will be assigned to any one individual as well as representative of the site-specific conditions under which an individual will be required to perform such duties. For example, the physical fitness test should consider the longest distance any one individual will be required to traverse before reaching a predetermined fighting position within the required response timeline assigned to that position; the nature of any obstacles, such as stairways, that any individual will have to negotiate; and the total weight of equipment that will have to be carried, etc. The physical fitness test should replicate these conditions (or an equivalent exertion) to ensure the

ability all individuals to respond to a security contingency event." Licensees may consider, if appropriate or desired, performance standards that are established and approved by local, state, or federal law enforcement agencies or US military services.

As described in Section VI, paragraph B.2.(a)(2) of Appendix B to 10 CFR Part 73, individuals assigned security duties and responsibilities shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities as identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

c) A training and qualification plan should describe the components of the physical fitness examination that the licensee administers to meet the above requirement.

d) The description of the physical fitness examination should be inclusive and contain a listing of each characteristic of the exam and should include the pass or fail criteria applied for each characteristic.

As described in Section VI, paragraph B.2.(a)(3) of Appendix B to 10 CFR Part 73, the physical examination required in paragraph B.2.(a)(2) must be administered by a licensed health professional with the final determination being made by a licensed physician to verify the individual's physical capability to perform assigned duties and responsibilities.

e) A training and qualification plan should describe the qualifications and criteria used to ensure that the licensed health care professional (e.g., a licensed physician's assistant) is a person qualified to asses determinations of endurance, stress, and musculoskeletal development associated with exertion and physical performance.

f) The final determination made to satisfy the above regulation is the final determination made by the licensed physician of individual suitability to perform security-related tasks, duties, and responsibilities.

As described in Section VI, paragraph B.2.(b)(1) of Appendix B to 10 CFR Part 73, each individual must meet vision requirements of not less than distant visual acuity in each eye, correctable to 20/30 (Snellen or equivalent) in the better eye and 20/40 in the other eye with eyeglasses or contact lenses.

g) A training and qualification plan should describe the vision testing process implemented by the licensee in making the vision acceptability determinations. The training and qualification plan describes the testing process implemented to ensure that vision is at least 20/40 in the individual's better eye and describes how the licensee ensures that the individual carries a second pair of corrective lenses if uncorrected distance vision is not 20/40 in the better eye. The training and qualification plan should describe the testing process to ensure that an individual's field of vision is at least 70 degrees horizontal meridian in each eye and describes the testing methodology to ensure an individual can distinguish red, green, and yellow. In addition, the training and qualification plan should confirm that glaucoma is a disqualifying condition unless controlled by medical or surgical means, describes those acceptable medical or surgical means, and describes the process implemented to ensure that medication authorized to treat glaucoma will not adversely affect an individual's ability to perform assigned security duties.

h) A training and qualification plan should describe the on-the-job evaluation process implemented by the licensee for evaluating mild color vision defects and describes the

process implemented to ensure that an individual's use of corrective eyeglasses or contact lenses will not interfere with the individual's ability to perform assigned duties and responsibilities.

As described in Section VI, paragraph B.2.(c)(1) of Appendix B to 10 CFR Part 73, individuals may not have hearing loss in the better ear greater than 30 decibels average at 500 Hz, 1,000 Hz, and 2,000 Hz with no level greater than 40 decibels at any one frequency.

i) A training and qualification plan should describe the hearing testing process implemented to ensure that individuals assigned security duties and responsibilities meet the above stated hearing requirements and describes the procedures implemented to evaluate the use of a hearing aid, should one be used to meet these requirements. The plan also describes the process implemented to ensure that a hearing aid, if used, does not decrease the individual's effective performance of assigned duties.

As described in Section VI, paragraph B.2.(d)(1) of Appendix B to 10 CFR Part 73, individuals may not have an established medical history or medical diagnosis of existing medical conditions which could interfere with or prevent the individual from effectively performing assigned duties and responsibilities.

j) A training and qualification plan should describe the process and procedures implemented to ensure that sufficient inquiry is conducted to ensure that individuals who will be assigned security duties and responsibilities do not have pre-existing conditions, or currently existing previously undiagnosed medical conditions, or pre-existing diagnosis of habitual alcoholism or drug abuse, that will prevent them from performing those assigned duties and responsibilities.

k) A training and qualification plan should describe the process and procedures implemented to ensure that any individual with a diagnosis of habitual alcoholism or drug use has completed a rehabilitation program and describes the form and content of program completion certification that the licensee has determined provides a reasonable degree of confidence in and individual's suitability to perform security-related duties and responsibilities.

As described in Section VI, paragraph B.2.(f) of Appendix B to 10 CFR Part 73, an individual who has been incapacitated due to a serious illness, injury, disease, or operation which could interfere with the effective performance of assigned duties and responsibilities shall, before resumption of assigned duties and responsibilities, provide medical evidence of recovery and ability to perform these duties and responsibilities.

l) A training and qualification plan should describe the procedures and processes that the licensee implements following an individual's period of extended absence for sickness or illness to ensure that the individuals knowledge, skills, and abilities have not been lost over time, and ensure that they are fully qualified on tasks to be performed before they are reassigned any security duties or responsibilities.

2.4 Psychological Qualifications

As described in Section VI, paragraph B.3.(a) of Appendix B to 10 CFR Part 73, armed and unarmed individuals shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.

a) A training and qualification plan should describe the processes, procedures, and mechanisms implemented to have individuals perform tasks, complete assignments, make decisions, and execute functions that provide the means to demonstrate their ability to successfully perform assigned duties and responsibilities.

As described in Section VI, paragraph B.3.(b) of Appendix B to 10 CFR Part 73, a licensed psychologist, psychiatrist, or physician able to identify emotional instability shall determine whether armed members of the security organization and alarm station operators have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

b) A training and qualification plan should describe the licensee's processes and procedures for the administration of its psychological assessment program. The processes and procedures should describe the testing vehicles applied and provide articulation of the basis for establishing testing cut-off values, as well as the implementation of the interview process, including the basis and protocols for face-to-face or video conference interviews.

c) A training and qualification plan should confirm that the person making the determination that an unarmed individual supporting the security program has no emotional instability has been professionally trained to make this determination.

2.5 Medical Examinations and Physical Fitness Qualifications

As described in Section VI, paragraph B.4.(a) of Appendix B to 10 CFR Part 73, armed members of the security organization shall be subject to a medical examination by a licensed physician to determine the individual's fitness to participate in physical fitness tests.

a) A training and qualification plan should describe the licensee's processes and procedures for obtaining and retaining written certifications of an individual's ability to participate in physical fitness tests and to meet the physical fitness requirements associated with the duties to which an individual may be assigned.

b) A training and qualification plan should describe how armed members of the security organization demonstrate their physical fitness for duties that they may be assigned to perform.

c) A training and qualification plan should describe the physical fitness test protocols that specifically address how an individual demonstrates an ability to perform duties and responsibilities to which they may be assigned when the performance of these duties and responsibilities are under conditions of strenuous activity, physical exertion, stress, and where appropriate, under conditions of exposure to the elements.

d) A training and qualification plan should describe how the licensee determines that an individual meets the physical attributes that demonstrate the necessary strength, endurance, and agility to perform consistent with assigned duties and how these attributes satisfy the performance objectives for implementing the licensee protective strategy during all operational conditions.

e) A training and qualification plan should describe the process the licensee implements to ensure that a qualified training instructor documents an individual's physical fitness qualifications and that a security supervisor attests to the completeness and accuracy of this documentation upon completion of the individual's training.

f) A training and qualification plan should describe the process the licensee implements to validate that the licensee's training instructors are qualified to conduct and administer the licensee's security training program and described the process that the licensee implements to ensure the continued qualification of its training instructors.

Section VI, paragraph B.4.(b) of Appendix B to 10 CFR Part 73, further requires that before assignment, armed members of the security organization must demonstrate the capability to perform assigned duties and responsibilities through the conduct of a practical physical fitness test.

g) A training and qualification plan should consider the physical conditions, such as strenuous activity, physical exertion, levels of stress, and exposure to the elements, that pertain to each individual's assigned security duties for both normal and emergency operations and describes the methodologies used to simulate site-specific conditions under which the individual will be required to perform assigned duties and responsibilities. These methodologies should include physical attributes and performance objectives which demonstrate the strength, endurance, and agility consistent with assigned duties during normal and emergency conditions. Methodologies used should replicate/simulate actual/equivalent stresses and physical exertion loads (heart rate, lung capacity) over a protracted amount of time to ensure that the physical fitness test provides a realistic indication that each individual has the requisite ability to perform the types of physical tasks that may be required if called upon to do so.

2.6 Physical Requalification

As described in Section VI, paragraph B.5.(a) of Appendix B to 10 CFR Part 73, at least annually, armed and unarmed individuals shall be required to demonstrate the capability to meet the physical requirements of this appendix and the licensee training and qualification plan.

a) A training and qualification plan should describe the process implemented at least annually by the licensee to ensure that each armed and unarmed individual who supports the security organization demonstrates the capability to meet the physical requirements to perform duties and responsibilities and implement assigned portions of the licensee's protective strategy. A training and qualification plan also should describe the requalification and certification process as provided in 2.4.h above.

2.7 Duty Training and Qualification Requirements

As described in Section VI, paragraph C.1. of Appendix B to 10 CFR Part 73, all personnel who are assigned to perform any security-related duty or responsibility shall be trained and qualified to perform assigned duties and responsibilities to ensure that each individual possesses the minimum

knowledge, skills, and abilities required to effectively carry out those assigned duties and responsibilities. As described in Section VI, paragraph C.1.a of Appendix B to 10 CFR Part 73, the areas of knowledge, skills, and abilities that are required to perform assigned duties and responsibilities must be identified in the licensee's Commission-approved training and qualification plan.

a) A training and qualification plan should describe the process that the licensee implements to ensure that each individual who will be assigned duties and responsibilities for implementing or supporting the licensee's protective strategy, including the proper use of all equipment or devices required, has been trained and qualified to perform those duties or responsibilities prior to the assignment to perform any such duty or fulfill and such responsibility.

b) Where the licensee elects to use the Systematic Approach to Training (SAT) methodology provided in RG 5.75, the training and qualification plan shall confirm that the licensee follows the SAT methodology, to include the retention of associated documentation.

2.8 On-the Job Training

As described in Section VI, paragraph C.2. of Appendix B to 10 CFR Part 73, the licensee training and qualification program must include on-the-job training performance standards and criteria to ensure that each individual demonstrates the requisite knowledge, skills, and abilities needed to effectively carry-out assigned duties and responsibilities in accordance with the Commission-approved security plans, licensee protective strategy, and implementing procedures before the individual is assigned the duty or responsibility.

a) A training and qualification plan should describe the construct and implementation of its on-the-job training program that has been designed to provide an individual with the opportunity to demonstrate their ability to effectively apply the knowledge, skills, and abilities learned to effectively perform assigned duties and responsibilities for implementing the licensee's protective strategy.

b) A training and qualification plan should describe the construct and implementation of the 40-hour on-the-job training program that allows individuals to demonstrate their ability to implement the requisite knowledge, skills, and abilities to effectively perform contingency duties and responsibilities that implement the licensee's contingency plan, protective strategy, and associated implementing procedures. A training and qualification plan should also describe the certification process as provided in 2.4.h above.

c) A training and qualification plan should include, but not be limited to, the licensee's detailed training attributes, component parts, considerations, and implementing characteristics and activities for each of the knowledge, skills, and abilities provided in Section VI, paragraph C.2.(c) of Appendix B.

2.9 Performance Evaluation Program

As described in Section VI, paragraph C.3.(a) of Appendix B to 10 CFR Part 73, licensees shall develop, implement, and maintain a performance evaluation program that is documented in procedures which describe how the licensee will demonstrate and assess the effectiveness of their onsite physical protection program and protective strategy, including the capability of the armed response team to carry

out their assigned duties and responsibilities during safeguards contingency events. The training and qualification plan shall reference the performance evaluation program and procedures.

a) A training and qualification plan should summarize the content of each of the procedures that the licensee applies in implementing its performance evaluation program.

2.10 Drill and Exercise Performance

As described in Section VI, paragraph C.3.(b) through (l) of Appendix B to 10 CFR Part 73, a performance evaluation program shall include procedures for the conduct of tactical response drills and force-on-force exercises designed to demonstrate and assess the effectiveness of the licensee's physical protection program, protective strategy and contingency event response by all individuals with responsibilities for implementing the safeguards contingency plan.

b) A training and qualification plan should summarize the content, objectives, and expected outcomes of each of the procedures that the licensee has developed and implemented for the conduct of tactical response drills and force-on-force exercises.

c) A training and qualification plan should describe how the licensee ensures that each tactical response drill or force-on-force exercise conforms to the licensee's physical security plan, safeguards contingency plan, protective strategy, and their associated implementing procedures.

d) A training and qualification plan should describe how the licensee develops scripts or scenarios for tactical response drills and force-on-force exercises, including and how the licensee ensures that the scripts or scenarios provide one or more challenges to the licensee's protective strategy and demonstrate participant mastery of required knowledge, skills, and abilities.

e) A training and qualification plan should describe how the licensee ensures that tactical response drills and force-on-force exercises are conducted under conditions that simulate site-specific conditions under which participants would be expected to demonstrate mastery of required knowledge, skills, and abilities related to individual and team performance. In order to achieve these objectives, the licensee's training and qualification plan should describe:

(1) the number of armed responders and armed security officers used as documented in the physical security plan, and should confirm that no more than this number may be used for each drill or exercise,
(2) how the licensee will minimize the number and effects of artificialities in the tactical response drills and force-on-force exercises, and
(3) how the licensee uses systems or methodologies that simulate the realities of armed engagement through visual and audible means to ensure credible, realistic implementation of the licensee's protective strategy.

f) A training and qualification plan should describe the process and procedures associated with documenting tactical response drills and force-on-force exercises, including documenting individual participation, and describe the process for conducting the post-drill or post-exercise critique.

g) A training and qualification plan should describe the process implemented by the licensee to document and examine the successes and failures associated with human performance, equipment, and drill or exercise planning or execution, and the processes associated with entering any deficiencies into the licensee's corrective action program and protecting this documentation as safeguards information, as necessary.

h) A training and qualification plan should describe the process implemented by the licensee to ensure that each member of the security organization who is assigned duties and responsibilities associated with the implementation of the licensee's protective strategy:

(1) participates quarterly in at least one tactical response drill, and
(2) participates annually in at least one force-on-force exercise.

i) A training and qualification plan should describe the process and procedures that the licensee has implemented to staff and train a mock adversary force that will be used as an aggressor to challenge the licensee's protective strategy, security personnel, command and control functions, and implementing procedures, consistent with the DBT described in 10 CFR 73.1(a)(1).

j) A training and qualification plan should describe the process and procedures the licensee has implemented to evaluate and challenge protective strategies through the conduct of tabletop exercises, as a supplement to the results of tactical response drills and force-on-force exercises. If the licensee employees computer modeling tools to better inform the protective strategy, the licensee should also describe how the tool informs corresponding or conforming changes to the training of personnel.

k) A training and qualification plan should describe the development and implementation of the licensee's drill and exercise controller training and qualification program to ensure that each controller has the requisite knowledge, skills, and experience to control and evaluate exercises, including such areas as the licensee's protective strategy, individual and team defensive and intercept actions, as well as weapons functionality, performance characteristics, and serviceability.

l) A training and qualification plan should describe the licensee's safety expectations and the safety standards implemented by the licensee for the conduct of drills and exercises.

As described in Section VI, paragraph C.3.(m) of Appendix B to 10 CFR Part 73, licensees shall develop and document multiple scenarios for use in conducting quarterly tactical response drills and annual force-on-force exercises. These scenarios must be designed to test and challenge any one or more components of the licensee's physical protection program and protective strategy. Each scenario must include the use of a different or unique target set(s), and varying adversary equipment, strategies, and tactics, to ensure that the culmination of all scenarios challenges all aspects the onsite physical protection program and protective strategy.

m) A training and qualification plan should describe the content of each of the licensee's documented drills or exercises. A training and qualification plan should also describe the process used to ensure that each drill or exercise is different from the others and that the entire physical protection program and all aspects of the protective strategy are challenged through the combination of all of the drills or exercises. Lessons learned from the use of computer modeling tools should be described where appropriate. The

implementing details of the structure of each drill or exercise should allow each drill participant and controller to understand:

(1) the prerequisites for the start of each drill or exercise;
(2) the initiating event or action for each drill or exercise;
(3) the logical execution on each drill or exercise;
(4) the actions to be taken to suspend a drill or exercise for remedial training;
(5) the protective strategy or performance objectives to be achieved that, when accomplished, determines the conclusion of the drill or exercise; and
(6) the actions to be taken to suspend or terminate a drill or exercise for safety reasons.

n) A training and qualification plan should describe each of the licensee's documented drills in specific terms that include:

(1) the selection of targets or target sets,
(2) the allowable adversary strategy and armament for each drill or exercise, and
(3) the allowable adversary tactics for each drill or exercise.

2.11 Duty Qualification and Requalification

As described in Section VI, paragraph D.1.(a) of Appendix B to 10 CFR Part 73, armed and unarmed individuals shall demonstrate the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

a) A training and qualification plan summarizes the content of the exams and confirms that the licensee's written exams include testing for every attribute of the training provided to implement the licensee's protective strategy, derived from the Commission-approved plans, and specifically includes testing to ensure individuals understand their responsibilities for the recognition and reporting of potential tampering with both safety and security systems.

b) A training and qualification plan describes the administration of the testing program and confirms that the licensee requires that each individual achieve a minimum score of not less than 80 percent on each exam, administered annually, for armed members of the security organization.

c) A training and qualification plan describes the hands-on performance demonstration, including the theory and learning objectives for each of the required knowledge, skills, and abilities that each armed and unarmed individual must complete in order to demonstrate mastery of each element of the knowledge, skills, and abilities required to implement the licensee's protective strategy.

d) A training and qualification plan confirms that each member of the security organization understands that an authorized representative of the Commission is authorized to require that a member of the security force demonstrate understanding and ability to perform any of the knowledge, skills, or abilities described in the Commission-approved training and qualification plan.

e) A training and qualification plan describes the annual requalification of all armed and unarmed individuals who support the licensee's protective strategy. A training and qualification plan also describes the requalification and certification process and schedules as provided in Section 2.1.g above.

2.12 Weapons Training

As described in Section VI, paragraph E.1.(b)(1) of Appendix B to 10 CFR Part 73, each armed member of the security organization shall be trained and qualified by a certified firearms instructor for the use and maintenance of each assigned weapon to include but not limited to, marksmanship, assembly, disassembly, cleaning, storage, handling, clearing, loading, unloading, and reloading.

a) A training and qualification plan should describe the licensee's weapons training program processes, the training topics detailed in implementing procedures and lesson plans, and provide descriptions of lesson plans that have been implemented for each aspect of the weapons training program to ensure that each armed member of the security organization has been provided with the knowledge, skills, and abilities to competently manage each assigned weapon. At a minimum, implementing procedures and lesson plans should cover the following training topics:
   (1) weapons familiarization;
   (2) mechanical disassemble and reassembly, in whole or in part;
   (3) weapons capabilities, including ammunition capabilities and cautions for consideration when weapons are discharged around operating or recently operating equipment;
   (4) the fundamentals of marksmanship with emphasis on combat situations, including the changes encountered between daytime and nighttime shooting conditions;
   (5) weapons cleaning processes and storage conditions (e.g., whether holstered or placed in a storage locker);
   (6) safe weapons handling processes and considerations;
   (7) weapons loading, unloading, clearing, and reloading processes and considerations;
   (8) managing the effects of stress during combat conditions;
   (9) weapons zeroing and sighting processes and procedures;
   (10) the fundamentals of target determination, acquisition, and engagement;
   (11) the processes for resolving weapons malfunctions; and
   (12) the theory, considerations, and practices for executing effective cover and concealment tactics.

b) A training and qualification plan should describe the certification and recertification process, procedures, and documentation collection and retention requirements implemented by the licensee to train and certify and retain certification documentation for each of the licensee's weapon types for each of the licensee's firearms training instructors. The training and qualification plan should confirm that each firearms instructor is recertified at least every third year.

c) A training and qualification plan should describe the process and procedures implemented by the licensee to ensure that each armed member of the security organization participates in an annual firearms familiarization training process.

d) A training and qualification plan should describe the procedures implemented by the licensee to ensure that each armed member of the security organization is cognizant of the state law(s) regarding deadly force in which the site is situated and that each armed member of the security organization possesses the knowledge, skills, and abilities to effectively implement the licensee's deadly force policy.

e) A training and qualification plan should describe the procedures implemented by the licensee to ensure that each armed member of the security organization participates in firearms range activities nominally every four months and describes the licensee's implemented processes to ensure each armed member of the security organization maintains their firearms qualifications.

2.13 Weapons Qualification and Requalification

As described in Section VI, paragraph F of Appendix B to 10 CFR Part 73, qualification firing must be accomplished in accordance with Commission requirements and the Commission-approved training and qualification plan for assigned weapons. The results of weapons qualification and requalification must be documented and retained as a record for tactical weapons qualification, firearms qualification courses, courses of fire, and firearms requalification.

a) A training and qualification plan should describe the processes and procedures that the licensee has implemented to identify each firearm that the licensee has placed in operation at the site to meet the performance objectives of its protective strategy.

b) A training and qualification plan should describe the processes and procedures that the licensee has implemented to ensure that its tactical training program conforms to the site-specific characteristics that the licensee has identified that establishes the performance objectives of its protective strategy. A training and qualification plan should describe, for example:

(1) lighting availability and the use of night vision assistance, as required;
(2) target determination, acquisition, and engagement from elevated shooting positions, both fixed and as they become available;
(3) target engagement based on available fields-of-fire;
(4) tactical maneuvers to improve field-of-fire options;
(5) cover and concealment options during normal and outage conditions; and
(6) tactical deployment considerations under changing conditions.

c) A training and qualification plan should describe each of the daylight qualification courses and night fire qualification courses that the licensee has designed and implemented, and describes the licensee's adopted standard (i.e., law enforcement or other nationally recognized standard) for developing each course for each weapon type deployed at the licensee site.

d) A training and qualification plan should describe the method developed and implemented by the licensee for scoring each weapons certification course. A training and qualification plan shall confirm that the minimum acceptable score for individual handgun and shotgun courses is 70 percent of the maximum obtainable score for these weapon types, at least 80 percent of the maximum obtainable score for individual semi-automatic weapons and enhanced weapons, and a minimum of 80 percent of the maximum obtainable score for each of the licensee's tactical qualification courses.

e) A training and qualification plan should uniquely describe the licensee's annual requalification processes and procedures if those are different from the processes and procedures used in the initial weapons qualifications.

f) A training and qualification plan should describe the remedial training process implemented by the licensee to resolve conditions associated with any individual failure to achieve the minimum score required for any weapons certification course.

g) A training and qualification plan should describe the process implemented by the licensee to document all weapons qualification activities, including remedial training and subsequent requalification efforts and outcomes, including entry of weapons qualification failures into the licensee's corrective action program.

2.14 Weapons, Personal Equipment and Maintenance

As described in Section VI, paragraph G of Appendix B to 10 CFR Part 73, the licensee shall provide armed personnel with weapons that are capable of performing the function stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures. The licensee shall ensure that each individual is equipped or has ready access to all personal equipment or devices required for the effective implementation of the Commission-approved security plans, licensee protective strategy, and implementing procedures.

a) A training and qualification plan should describe the process and procedures implemented by the licensee to ensure that every member of the security organization assigned duties and responsibilities for implementing the licensee's protective strategy has been provided with the weapons necessary to implement that strategy.

b) A training and qualification plan should describe the process and procedures implemented to ensure that all members of the security organization are issued or have ready access to all equipment necessary for the implementation of the licensee's protective strategy. A training and qualification plan should confirm by reference or by list that, at a minimum, the equipment described in Section VI, paragraph G.2.(b) of Appendix B to 10 CFR Part 73, is available for armed members of the security organization at all times and in quantities necessary for the implementation of the licensee's protective strategy.

c) A training and qualification plan should describes the licensee's firearms maintenance program implementation, including:

(1) the procedures implemented for conducting weapons test firing, to include accuracy and functionality,
(2) the procedures for confirming the operational functionality of each weapon,
(3) the procedures that describe the proper cleaning and individual maintenance activities to be performed by members of the security organization,
(4) the procedures that describe the firearms program documentation,
(5) the procedures and processes that describe the control and accountability of all weapons and ammunition on the licensee's site,
(6) the procedures that address the storage of firearms that are issued to individuals from an armory or other security operations controlled environment

(7) the procedures that address the storage of readily available firearms at appropriately secured remote locations that provide access for tactical acquisition, and
(8) the process and procedures for members of the security organization to become certified as an armorer and to retain the armorer certification.

2.15 Records and Reviews

The provisions of Section VI, paragraph H of Appendix B to 10 CFR Part 73, require that the licensee shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of 10 CFR 73.55(q). Section VI, paragraph C.2.(b) of Appendix B to 10 CFR Part 73 requires that a qualified training instructor document an individual's on-the-job training. The documentation that is created by the licensee training instructor to record the successful completion of required on-the-job training elements (i.e., the data and test results that were achieved by the individual for each required task, to include signatures and initials of the trainee and training instructor) must be retained as part of the "Initial Qualification Record" (IQR) in accordance with 10 CFR Part 73, Appendix B. This documentation must be retained by the licensee in accordance with 10 CFR 73.55(q) and 10 CFR 73, Appendix B.VI., Section H.1, even if the licensee summarizes the information in another record. Consistent with Section VI, paragraph H.2 of Appendix B to 10 CFR Part 73, the IQR must be retained for three years after termination of the individual's employment and the licensee shall retain each requalification record for three years after it is superseded.

a) A training and qualification plan should describe the licensee's data collection and record retention process and procedures that, at a minimum, conform to the requirements in Section VI, paragraph H of Appendix B to 10 CFR Part 73.

b) A training and qualification plan should describe the process and procedures that the licensee has implemented to conduct training and qualification program reviews as required by 10 CFR 73.55(m).

3. Nuclear Power Reactor Safeguards Contingency Plans

As described in 10 CFR 73.55(c)(5), the licensee shall establish, maintain, and implement a Safeguards Contingency Plan that describes how the criteria set forth in Section II of Appendix C to 10 CFR part 73, "Nuclear Power Plant Safeguards Contingency Plans," will be implemented.

3.1 Introduction

As described in Section II, paragraph A of Appendix C to 10 CFR Part 73, the safeguards contingency plan is a documented plan that describes how licensee personnel implement the licensee's physical protection program to defend against threats to the licensee facility, up to and including the DBT of radiological sabotage. The goals of the licensee safeguards contingency plan are:

a) To organize the response effort at the licensee level;
b) To provide predetermined, structured response by licensees to safeguards contingencies;

c) To ensure the integration of the license response by other entities, such as local law enforcement personnel of offsite fire protection personnel; and

d) To achieve a measurable performance in response capability.

To achieve these objectives, the licensee's safeguards contingency plan should describe the interactions between this plan, the physical security plan, and the training and qualification plan to include how these plans are integrated to provide a physical protection program. The plan should identify and define the objectives to be accomplished and site-specific actions to be taken, including the identification of participant's responsibilities, in the event of threats or sabotage that could directly or indirectly endanger the public health and safety or common defense and security. In addition, the evaluation, validation, and testing of the implementation of this plan should be conducted in accordance with Appendix B to 10 CFR Part 73. The safeguards contingency plan implementation requirements should also be coordinated sufficiently to ensure that the implementation of emergency plans developed under Appendix E to 10 CFR Part 50 remains effective.

Licensees should ensure that interactions between security personnel and other site personnel, as described in 10 CFR 73.58, remain coordinated and are effectively implemented. Licensees should apply the guidance found in RG 5.74 to support achieving this objective.

3.2 Contents of the Plan

As described in Section II, paragraph B of Appendix C to 10 CFR Part 73, each safeguards contingency plan shall include five categories of information: Background, Generic Planning Base, Licensee Planning Base, Responsibility Matrix, and Implementing Procedures.

Licensees may choose to address these categories separately or as combined topics in their individual plans; however, each category shall be addressed.

a) Background

This category of information shall identify the perceived dangers and incidents that the plan will address and provide a general description of how a response is organized.

(1) Perceived Danger

Consistent with the DBT specified in 10 CFR 73.1(a)(1), the licensee shall identify and describe within their safeguards contingency plan the perceived dangers, threats, and incidents against which the contingency plan is designed to protect. The licensee should consider information received from local, state, and federal organizations regarding potential threats as applicable in safeguards contingency planning.

(2) Purpose of the Plan

The licensee's safeguards contingency plan shall describe the general goals, objectives, and operational concepts underlying the implementation of approved safeguards contingency plan. The safeguards contingency plan should include a description of how the licensee accomplishes specific, defined objectives in the event of a threat of radiological sabotage that could directly or indirectly endanger public health and safety.

(3) Scope of the Plan

The licensee's safeguards contingency plan delineates how the onsite security response effort is organized and coordinated to effectively respond to a safeguards contingency event. The licensee should include the command and control protocols that ensure the coordinated and integrated response of other onsite disciplines as well as responding offsite agencies, to emergency conditions resulting from a safeguards contingency event. This section of the safeguards contingency plan also should describe how the response to safeguards contingency events has been integrated in other site emergency response procedures to ensure that the security response identified in the safeguards contingency plan does not conflict with the implementation of other site emergency procedures.

(4) Definitions

The licensee's safeguards contingency plan contains a list of terms and their definitions used in describing operational and technical aspects of the approved plan. This list should be in accordance with, or supplement, terms used in the licensee's site security plan and training and qualification plan. A licensee may choose to submit its physical security plan, training and qualification plan, and safeguards contingency plan as a single document that contains an aggregate definitions section for all three plans.

b) Generic Planning Base

This category of information shall define the criteria for initiation and termination of responses to security events to include specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved safeguards contingency plan. As described in Section II, paragraph B.2 of Appendix C to 10 CFR Part 73, the licensee's generic planning base must:

(1) Identify those events that will be used for signaling the beginning or aggravation of a safeguards contingency event according to how they are perceived initially by the licensee's personnel. The licensee's safeguards contingency plan and implementing procedures should identify the characteristics that meet thresholds for considering that a condition is escalating and the response measures to be implemented when these conditions have been met. Licensees shall ensure detection of unauthorized activities and shall respond to all alarms or other indications signaling a security event, such as a penetration of a protected area, vital area, or unauthorized barrier penetration by a vehicle or a person; tampering; bomb threats; or other threat warnings either verbal (e.g., telephoned threats) or implied (e.g., escalating civil disturbance).

(2) Define the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency event to prepare for further responses, to establish a level of response preparedness, or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency. The identification of specific objectives to be accomplished and the initial and follow-on actions to be implemented to achieve those objectives, including the point at which the contingency action may be terminated, should be

contained in licensee's safeguards contingency plan and implementing procedures.

(3) Identify the data, criteria, procedures, mechanisms, and logistical support necessary to achieve the objectives. The specific implementation details involving the collection of data, the specific attributes of decision making criteria, details of and deployment of mechanisms and resources, and the processes for determining the entry of logistical support should be contained in licensee's safeguards contingency plan implementing procedures.

The following are examples of situations that should be addressed in the licensee safeguards contingency plan. These examples should not be considered all inclusive, rather, they should be considered as a framework that would typically apply to all licensees. Licensees may have additional unique site-specific considerations that they may address in a manner that is different than the situations addressed in this guidance. Each of the following event descriptions include a brief overview of high level response objectives and the preliminary data that may be needed to effectively respond. The details of decisions and actions that are necessary to respond to each event should be presented in a manner that describes the licensee's implementation of actions designed to meet the requirements above in Items 1 through 3, and incorporated into the responsibility matrix required by Section II, paragraph B.4 of Appendix C to 10 CFR Part 73, and licensee safeguards implementing procedures.

EVENT 1: MALEVOLENT THREAT/USE OF A VEHICLE

The threat of the malevolent use of a vehicle (vehicle bomb or use of vehicles in an attack) could be expressed by any communication pathway. Threats may be directly received by the licensee or indirectly provided through a law enforcement agency, mass media, external organization, or other party. Threats also may be perceived from indirect evidence by facility personnel, offsite authorities, or other parties who may notify facility management of the concern. The licensee could also receive notification of a vehicle bomb threat from the NRC. Notifications from the NRC may be received in a timeframe which would allow a timely and orderly deployment of additional contingency barriers/roadblocks and implementation of steps to ensure facility and personnel safety. If the event is determined to be a credible threat, actions to stop or interdict the threat would be implemented as described in the safeguards contingency plan and licensee implementing procedures. If a malevolent use of a vehicle occurs, this event should be managed as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 2: DETECTION OF IMPENDING ATTACK, THREAT/DIRECT ARMED ATTACK

The threat of an impending attack or direct armed attack could be expressed by any communication pathway. Threats may be directly received by the licensee or indirectly provided through a law enforcement agency, mass media, external organization, or other party. Threats also may be perceived from indirect evidence by facility personnel, offsite authorities, or other parties who may notify facility management of their concern. The identification of a direct armed attack may occur with an alarm at a point along the protected area or be discovered through closed circuit television (CCTV) surveillance by CAS or SAS operators. Upon any determination that an armed attack, hostile intrusion, or violation of a protected area or vital area barrier is

underway or is expected, actions to reduce vulnerability, interdict, and neutralize the event should be implemented as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 3: CIVIL DISTURBANCE

A civil disturbance is typically a group of persons overtly protesting facility operations or activities. Peaceful or otherwise passive demonstrations are not civil disturbances. Civil disturbances do not involve individuals within the group participating in hostile, aggressive, or dangerous actions. Licensees should ensure that actions are implemented to monitor the behavior of the participants, request offsite assistance, adjust the security profile as necessary to ensure the integrity of the facility perimeter, and minimize vulnerability to the facility and to facility employees. Upon any determination that a civil disturbance is expected, actions to reduce vulnerability should be implemented as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 4: OWNER CONTROLLED AREA, PROTECTED AREA, OR VITAL AREA INTRUSION/DISCOVERY OF BREACHED BARRIER

An OCA, protected area, or vital area intrusion would typically be identified with initiation of an alarm at the affected zone or barrier, or notification from personnel such as a security patrol (or, in the case of the OCA, through an Early Warning System, if used). Breached barriers would be revealed through CCTV observation, investigation by a security officer responding to an alarm annunciation, or reported by other facility personnel. Information regarding a breach could be received by telephone, radio, facility intercom, or in person. Any confirmed barrier breach as evidenced by barrier damage from apparent forced entry, video capture review, or direct observation by a security officer should be managed as described in the licensee safeguards contingency plan and implementing procedures. Any intrusion confirmed by a security officer, CCTV observation, or other facility personnel should be managed as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 5: FIRE, EXPLOSION, OR OTHER CATASTROPHE

A fire, explosion, or other catastrophe could be identified with the initiation of a local alarm and reported by facility personnel or discovered by security while on patrol. Reports of such events could be by telephone, radio, facility intercom, or in person. Any fire, explosion, or other catastrophic event should be immediately evaluated for the potential to be a contingency event. If determined to be other than accidental, the event should be managed as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 6: DETECTION OF ABERRANT BEHAVIOR

Detection of aberrant behavior within the protected area or a vital area could be made through visual observation by facility or security personnel. The event could be reported by telephone, radio, facility intercom, or in person. A verbal or physical confrontation between individuals that does not present a risk to nuclear safety would not constitute a security condition or hostile action but may be a fitness for duty event that would be resolved by implementing the requirements of the licensee's behavior observation program. In the event that responding security personnel determine that the event is outside the scope of the behavior observation program and should be considered a contingency event, the licensee should then manage the condition as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 7: SECURITY FORCE STRIKE OR UNAVAILABILITY OF SECURITY FORCE

A security force strike would typically be an action that the licensee could prepare for and therefore implement pre-planned compensatory actions. Such a situation could be predicted based upon planned or ongoing labor negotiations. A spontaneous security force strike without prior warning, while unlikely, should be considered by the licensee with compensatory measures identified and addressed in the licensee safeguards contingency plan with full implementation details in the licensee implementing procedures. The licensee should then be prepared to manage either a pre-planned or spontaneous labor strike, or other personnel unavailability condition, as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 8: LOSS OF CONTACT WITH SECURITY OFFICERS

Loss of contact with a security officer may be due to an incapacitating personal injury, an incapacitating medical condition, or a hostile act. The loss of contact with a security officer is an immediate contingency event until determined otherwise. Loss of contact with a security officer could be a precursor of an attack or other adversary action. Loss of contact would typically be discovered when the CAS or SAS attempts to establish contact with a security officer and the officer fails to respond. Loss of contact could also be discovered when a security officer fails to report during a pre-scheduled communications check. If this event is determined to be a hostile action, it should be reported to the Shift Manager and the licensee should transfer to the applicable security event. The licensee should manage either of these loss-of-contact conditions as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 9: CONFIRMED SABOTAGE, TAMPERING, VANDALISM, MALICIOUS MISCHIEF

An act of or potential act of sabotage, tampering, vandalism, or malicious mischief directed against licensee facility safety or security could be expressed by any communication pathway. Such an act could also be discovered by security officers on patrol, CCTV assessment, facility personnel, or reported to a licensee through a law enforcement agency. Vandalism may be severe enough to cause conditions that should be considered as a contingency event. Malicious mischief alone typically will not meet the criteria for a contingency event or hostile action. An actual act of sabotage should be considered a contingency event until the licensee has determined that the conditions lack

the significance to warrant a continued contingency response. A potential act of sabotage should be investigated and acted upon as a contingency event or resolved as a non-contingency event. Licensees should be guided in part by Information Notice No. 96-71, "Licensee Response to Indications of Tampering, Vandalism, or Malicious Mischief (Ref. 28)," in the development of their safeguards contingency plans. The licensee should manage either of these conditions as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 10: BOMB THREAT/EXPLOSIVE DEVICE DISCOVERED

A bomb threat or the discovery of a suspected explosive device could be reported by any communication pathway. Bomb threat notifications could be received by the licensee from a local, state, or federal law enforcement agency, or from the NRC. Any report of an explosive device should be treated as a contingency event until the licensee has determined that the threat is not credible. The discovery of a suspected explosive device should be treated as a contingency event until the licensee has determined that the object reported is not an explosive device. The licensee should manage either of these conditions as described in the safeguards contingency plan and licensee implementing procedures.

EVENT 11: LOSS OF ONSITE/OFFSITE SECURITY COMMUNICATIONS SYSTEMS

The discovery of the loss of any licensee communication system relied upon to implement the licensee's protective strategy should be considered a significant event and immediately investigated in order to determine whether the loss of the communication system is due to a mechanical or electrical failure that either is or is not a threat. Consequently, all remaining communications systems relied upon to implement the licensee's protective strategy should be checked immediately as well, and appropriate compensatory measures implemented in accordance with the licensee's physical security plan. A licensee discovery that any communication system failure was the result of an intentional or hostile act should manage the loss of communications as a contingency event as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 12: LOSS OF SECURITY SYSTEM POWER

The loss of security system power would typically be identified in the CAS or SAS, or by security officers on patrol. A failure of the emergency backup system to restore power would also be identified in the CAS or SAS. The loss of any licensee security system power supply relied upon to implement the licensee's protective strategy should be considered a significant event and immediately investigated in order to determine whether the loss of power is due to a mechanical or electrical failure that either is or is not a threat and appropriate compensatory measures should be implemented in accordance with the licensee's physical security plan. A licensee discovery that any security system power failure was the result of an intentional or hostile act should manage the loss of power as a contingency event as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 13: LOSS OF ALARM ASSESSMENT SYSTEM OR IDS

The loss of the alarm assessment system or IDS would typically be identified by the CAS or SAS when an unexpected annunciation failure occurs or when an expected annunciation failure occurs during surveillance or performance testing. Loss of alarm assessment or IDS should be considered a significant event and immediately investigated in order to determine whether the loss of alarm assessment or IDS is due to a mechanical or electrical failure that either is or is not a threat and appropriate compensatory measures implemented in accordance with the licensee's physical security plan. A licensee discovery that any loss of alarm assessment or intrusion detection was the result of an intentional or hostile act should manage the loss of power as a contingency event as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 14: LOSS OF SECURITY LIGHTING

The loss of security lighting would typically be identified by the CAS or SAS or by security personnel on patrol. Loss of security lighting should be considered a significant event and immediately investigated in order to determine whether the loss of security lighting is due to a mechanical or electrical failure that either is or is not a threat and appropriate compensatory measures implemented in accordance with the licensee's physical security plan. A licensee discovery that any loss of security lighting was the result of an intentional or hostile act should manage the loss of power as a contingency event as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 15: LOSS OF SECURITY COMPUTER

The loss of the security computer system would typically be identified by the CAS or SAS. Loss of the security computer system should be considered a significant event and immediately investigated in order to determine whether the loss of the security computer system is due to a mechanical or electrical failure that either is or is not a threat and appropriate compensatory measures implemented in accordance with the licensee's physical security plan. A licensee discovery that any loss of the security computer system was the result of an intentional or hostile act should manage the loss as a contingency event as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 16: EXTORTION/COERCION/HOSTAGE THREAT

An extortion, coercion, or hostage threat could be reported by any communication pathway. Existence of or the potential for these threats may be received through local, state, or federal law enforcement agencies, or through the NRC. Threats of this nature may also be provided directly or indirectly by or through facility personnel. Any threat associated with an extortion or coercion to take some act against the licensee's facility or personnel, or any hostage threat against a member of the facility, should be considered significant and immediately investigated in order to determine the credibility or validity of the threat. If the investigation determines that the event is in progress and may result in a degradation to the safety or security of the facility or personnel, the licensee should manage the situation as a contingency event as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 17: WATERBORNE THREAT

A waterborne threat could be discovered by patrols or detection technologies utilizing any communication pathway. Existence of or the potential for a waterborne threat may be received through local, state, or federal law enforcement agencies, or through the NRC, Coast Guard, or facility personnel. A credible threat of a waterborne attack should be managed through appropriate compensatory measures implemented in accordance with the licensee's physical security plan and as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 18: COORDINATED LAND VEHICLE BOMB ATTACK

A coordinated land vehicle bomb attack would typically be identified by: CCTV observation in the OCA, initiation of an alarm at an affected zone, the breach of a barrier that activates a component of the IDS, observation by a patrolling security officer, or reported by other facility personnel. Reports of an attack could be received by any communication pathway or by explosion. Information that establishes a coordinated land vehicle bomb attack is imminent or underway should be considered significant and immediately investigated in order to determine the credibility or validity of the threat. If the investigation determines that the information is credible, the event should be managed through appropriate compensatory measures implemented in accordance with the licensee's physical security plan and as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 19: STANDOFF ATTACK BY A SNIPER

Notification of threats of an impending standoff attack, such as a sniper attack, may be provided through local, state, or federal law enforcement agencies, some other party, or through the NRC. Any threat of a sniper attack should be considered significant and immediately investigated in order to determine the credibility or validity of the threat. If the investigation determines that the information is credible, the event should be managed through appropriate compensatory measures implemented in accordance with the licensee's physical security plan and as described in the licensee safeguards contingency plan and implementing procedures. In the event that the licensee is the subject of an in-progress sniper attack, the event should be managed through appropriate compensatory measures implemented in accordance with the licensee's physical security plan and as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 20: INSIDER THREAT

A trusted person with protected or vital area access, or access to digital computer and communications systems and networks from outside the protected area, can pose a significant threat to the safety and security of a licensee facility. Mitigation of opportunities for insider tampering is particularly important because an insider may have knowledge of how to manipulate various systems in ways that are difficult to detect. Indications of an insider action may come from a significant variety of circumstance or conditions. In the event that the licensee is the subject of an insider attack, the event should be managed as described in the licensee safeguards contingency plan and implementing procedures.

EVENT 21: ATTEMPTED OR CONFIRMED CYBER ATTACK

Identification of an attempted of confirmed cyber attack could come as a result of a recognized compromise of a critical digital asset or system that supports safety related or important to safety functions, security functions, emergency preparedness functions, or support systems that if compromised, would adversely impact facility safety, security, or emergency preparedness. In the event that the licensee is the subject of a cyber attack, the event should be managed as described in the licensee cyber security plan and implementing procedures. At a minimum, the licensee should determine the credibility and scope of the threat to the facility as a result of a cyber attack and if a security condition has occurred, communicate the determination to the Shift Manager. Licensees should review RG 5.71 for additional guidance.

c) Licensee Planning Base

This category of information shall include factors affecting safeguards contingency planning that are specific for each facility. To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they may be incorporated by reference in the safeguards contingency plan. As described in Section II.B.3 of Appendix C to 10 CFR Part 73, the licensee's licensee planning base must address:

(1) Organizational Structure

As described in Section II.B.3.a. of Appendix C to 10 CFR Part 73, the licensee safeguards contingency plan must describe the organization's chain of command and delegation of authority during safeguards contingency events, to include a general description of how command and control functions will be coordinated and maintained.

Licensees should provide specific positions and titles of the persons initially responsible for a decision making process and include the position and title of the person(s) to whom delegation would flow and under what circumstances. The description of the command and control function should define the command and control function during normal operations and describe how that function changes during a contingency event, to include an articulation of the means of coordination and maintenance of the command and control function as the licensee progresses through a contingency event.

(2) Physical Layout

As described in Section II.B.3.b. of Appendix C to 10 CFR Part 73, the licensee safeguards contingency plan must include a site map depicting the physical structures located on the site, including onsite independent spent fuel storage installations, and a description of the structures depicted on the map.

Plans must also include a description and map of the site in relation to nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Descriptions and maps must indicate main and alternate entry routes for law enforcement or other offsite response and support agencies and the location for marshaling and

coordinating response activities. Providing information that meets the requirements described in Section II.B.3.b. of Appendix C to 10 CFR Part 73 can be accomplished in segments that can be assembled to provide a clear view and understanding of the entire physical layout. The NRC recognizes that a single map or drawing that would contain all the information required may become too cluttered to be clearly understood. Descriptions of alternate entry routes for law enforcement and other offsite response and support may be brief but these routes should be clearly recognizable. Locations for marshaling and coordinating response activities should be clearly distinguished.

(3) Safeguards Systems

As described in Section II.B.3.c. of Appendix C to 10 CFR Part 73, the licensee safeguards contingency plan must include a description of the physical security systems that support and influence how the licensee will respond to an event in accordance with the design basis threat described in 10 CFR 73.1(a).

The licensee's description shall begin with onsite physical protection measures implemented at the outermost facility perimeter, and must move inward through those measures implemented to protect target set equipment. This description should include, but is not limited to, components such as alarm station consoles, physical barriers, early warning systems, alarm systems, access control devices and measures, surveillance capabilities, and communications systems with both primary and backup systems. Licensees should clearly articulate the measures that are in place in the OCA and migrate this articulation to the protected area fencing. Licensees should articulate the migration from the protected area fence into the protected area and into vital areas as applicable.

A. Physical security systems and security systems hardware to be discussed include security systems and measures that provide defense-in-depth (i.e., physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems). Licensees should provide specific information for each of the required attributes that provide the defense-in-depth for physical security systems and hardware.

B. The specific structure of the security response organization to include the total number of armed responders and armed security officers documented in the approved security plans as a component of the protective strategy and a general description of response capabilities shall also be included in the licensee safeguards contingency plan. The security response organization is composed of all security personnel except unarmed escort personnel and unarmed watchpersons. Licensee security management, security supervisors, and alarm station operators are all considered members of the response organization. Armed responders and armed security officers should be identified by the total number of armed personnel credited by the licensee for implementing the licensee's protective strategy.

C. Licensees shall ensure that individuals assigned duties and responsibilities to implement the licensee safeguards contingency plan are trained and qualified in those duties according to the Commission-approved security plans, and the performance evaluation program. Licensees should describe the process(s)

applied to ensure that only trained and qualified personnel are assigned duties or responsibilities to implement the licensee safeguards contingency plan and how these personnel are assessed through the performance evaluation program.

D. Armed responders shall be available to respond from designated areas inside the protected area at all times and may not be assigned any other duties or responsibilities that could interfere with assigned armed response team duties and responsibilities. Licensees should describe the typical staging of armed responders inside the protected area by location and number, and the process(s) applied to ensure that personnel are not assigned duties that would interfere with executing their response team duties.

E. Licensees shall develop, implement, and maintain a written protective strategy to be documented in procedures that describe in detail the physical protection measures, security systems, and deployment of the armed response team relative to site-specific conditions, to include but not be limited, to facility layout, and the location of target set equipment and elements. The protective strategy should support the general goals, operational concepts, and performance objectives identified in the licensee's safeguards contingency plan. The protective strategy should :

i. Be designed to meet the performance requirements and objectives of 10 CFR 73.55(a) through (k).
ii. Identify predetermined actions, areas of responsibility, and timelines for the deployment of armed personnel.
iii. Contain measures that limit the exposure of security personnel to possible attack, including incorporation of bullet resisting protected positions and the use of personal protective equipment, such as bullet-resisting vests and gasmasks.
iv. Contain a description of the physical security systems and measures that provide defense-in-depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.
v. Describe the specific structure and responsibilities of the armed response organization to include: (1) the designated minimum number of armed responders necessary to prevent significant core damage and spent fuel sabotage who are available at all times inside the protected area, (2) the number of armed security officers designated to augment armed responders within pre-determined timelines, (3) the number of armed security officers designated to strengthen onsite response capabilities and who are available onsite at all times, and (4) the total number of armed responders and armed security officers documented in the approved security plans as a component of the licensee protective strategy.
vi. Provide a command and control structure, to include response by offsite law enforcement agencies, which ensures that decisions and actions are coordinated and communicated in a timely manner to facilitate response.

Licensees should consult RG 5.76 and RG 5.69 for additional guidance on the specific level of detail that should be in the licensee safeguards contingency plan and implementing procedures.

(4) Law Enforcement Assistance

As described in Section II.B.3.d. of Appendix C to 10 CFR Part 73, licensees shall provide a listing of the available law enforcement agencies, a general description of their response capabilities and their criteria for response, and a discussion of working agreements or arrangements for communicating with these agencies.

An acceptable method for meeting this requirement is the coordinated development of a written law enforcement response plan between the licensee and supporting local, state, or federal law enforcement agencies. Coordination of personnel and physical assets and communication protocols between the licensee and law enforcement agencies expected to respond to the site during a contingency event should be documented in this plan. During the planning for law enforcement response, licensees should consider the potential impacts of a law enforcement response on the site emergency plan and the potential for adverse impacts to operational considerations. Agreements between the licensee and supporting law enforcement agencies should address the periodicity on which these plans will be tested, drilled, and exercised.

(5) Policy Constraints and Assumptions

As described in Section II.B.3.e. of Appendix C to 10 CFR Part 73, the safeguards contingency plan shall contain a discussion of State laws, local ordinances, and company policies and practices that govern licensee response to incidents. The safeguards contingency plan must include, but is not limited to, the following:

A. Use of Deadly Force

The licensee safeguards contingency plan should include the basis for the licensee's position on the use of deadly force. The basis the licensee applies would typically be the underlying state laws regarding the use of deadly force. Licensee basis should be modeled after the use of deadly force policies of state and local law enforcement programs.

B. Recall of Off-Duty Employees

The licensee policy regarding the recall of security personnel in an emergency should be provided in the licensee safeguards contingency plan. The details of the expected recall process execution for security personnel should be in licensee implementing procedures. Licensees should consider modeling the recall process for security personnel with the recall process for site operations personnel described in the licensee's emergency plan.

C. Site Jurisdictional Boundaries

The jurisdictional boundaries provided in the licensee's safeguards contingency plan should have been included as components of meeting the requirements described in Section 3.2.c.(2) above. However, if the licensee has not included a clearly defined site description that includes the site jurisdictional boundaries, these boundaries shall be provided here, as described in Section II.B.3.e. of Appendix C to 10 CFR Part 73.

D. Use of Enhanced Weapons, If Applicable

In the event the licensee is authorized by the Commission under Section 161A of the Atomic Energy Act of 1954, as amended, and has deployed enhanced weapons at their facility, the licensee safeguards contingency plan should describe the function that these enhanced weapons perform in support of the protective strategy.

The safeguards contingency plan should also include a discussion of the following, if applicable:

E. Preemption Authority

Under Section 161A of the Atomic Energy Act of 1954, as amended, the Commission may authorize licensee personnel to transfer, receive, possess, transport, import, and use handguns, rifles, shotguns, semi-automatic assault rifles, enhanced weapons (short-barreled shotguns, short-barreled rifles, and machineguns), ammunition for any such weapon, and large capacity ammunition feeding devices, notwithstanding state and local firearms laws, including regulations, that prohibit such conduct. Where granted by the Commission, the licensee should identify and reference the licensing document through which the licensee is granted this authority, provide a general description of state or local laws to which preemption authority is applied, and provide a description of how preemption authority is implemented at the site.

(6) Administrative and Logistical Considerations

As described in Section II.B.3.f. of Appendix C to 10 CFR Part 73, the descriptions of licensee practices which influence how the security organization responds to a safeguards contingency event should include, but are not limited to, a description of the procedures that will be used for ensuring that equipment needed to facilitate response will be readily accessible, in good working order, and in sufficient supply.

Licensee safeguards contingency plans should describe the licensee response to each of the safeguards contingency events identified in Section 3.2.b.(3) above. Licensees should identify the procedures employed in responding to safeguards contingency events in their safeguards contingency plan and provide a purpose and objective for each procedure. Consistent with Section II.B.5.(iii) of Appendix C to 10 CFR Part 73, the procedures themselves are

considered implementing procedures and do not need to be submitted to the Commission for review and approval, but are subject to inspection by NRC staff.

d) Responsibility Matrix

This category of information consists of the detailed identification of responsibilities and specific actions to be taken by licensee organizations and/or personnel in response to safeguards contingency events.

As described Section II.B.4. of Appendix C to 10 CFR Part 73, licensees shall develop site procedures that consist of matrixes detailing the organization and/or personnel responsible for decisions and actions associated with specific responses to safeguards contingency events. The responsibility matrix and procedures shall be referenced in the licensee safeguards contingency plan.

As described in Section II.B.4.b. of Appendix C to 10 CFR Part 73, the responsibility matrix procedures shall be based on the events outlined in the licensee's Generic Planning Base and must include the following information:

(1) The definition of the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses, to establish a level of response preparedness, or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.
The licensee responsibility matrix should describe the various initiating events that could form the basis for a contingency response and describe the means or characteristics of conditions that would form a basis for escalation or de-escalation actions that should be undertaken.

(2) A tabulation for each identified initiating event and each response entity which depicts the assignment of responsibilities for decisions and actions to be taken in response to the initiating event.
The responsibility matrix should define the title of the response entity and the expected actions to be undertaken by each response entity for each postulated contingency event.

(3) An overall description of response actions and interrelationships specifically associated with each responsible entity must be included.
The responsibility matrix should define and describe each of the response actions to be undertaken by each of the persons executing actions and fulfilling responsibilities for each type of contingency event.

As described in Section II.B.4.c. of Appendix C to 10 CFR Part 73, responsibilities shall be assigned in a manner that precludes conflict of duties and responsibilities that would prevent the execution of the licensee safeguards contingency plan and emergency response plans.

(4) Licensees shall ensure that predetermined actions can be completed under the postulated conditions.

(5) Licensees should develop exercises that validate the predetermined actions provided in the responsibility matrix and evaluate these exercises as part of the licensees' performance evaluation program.

e) Implementing Procedures

As described in Section II.B.5. of Appendix C to 10 CFR Part 73, licensees shall establish and maintain written implementing procedures that provide specific guidance and operating details that identify the actions to be taken and decisions to be made by each member of the security organization who is assigned duties and responsibilities required for the effective implementation of the security plans and the site protective strategy.

(1) Licensees should ensure that implementing procedures accurately reflect information contained in the Responsibility Matrix required by Appendix C to 10 CFR Part 73, their security plans and other site implementing procedures.

3.3 Records and Reviews

a) Consistent with 10 CFR 73.55(m), licensees shall periodically conduct an audit of the effectiveness of the safeguards contingency plan.

b) The safeguards contingency plan audit must include a review of applicable elements of the physical security plan, training and qualification plan, implementing procedures and practices, the site protective strategy, and response agreements made by local, state, and federal law enforcement agencies.

c) Licensees shall retain all reports, records, or other documentation required by Appendix C, Section II. C, and in accordance with the requirements of 10 CFR 73.55(q).

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[3] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC staff complies with 10 CFR 50.109, "Backfitting," and any applicable finality provisions in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

Use by Applicants and Licensees

Applicants and licensees may voluntarily[4] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

Licensees may use the information in this regulatory guide for actions which do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59, "Changes, tests, and experiments." Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

Use by NRC Staff

The NRC staff does not intend to or approve of any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this regulatory guide, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request licensees to voluntarily adopt this regulatory guide to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action which would require the use of this regulatory guide. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this regulatory guide, generic communication, or promulgation of a rule requiring the use of this regulatory guide without further backfit consideration.

During regulatory discussions on plant- or site-specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this regulatory guide, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this regulatory guide are part of the licensing basis of the facility. However, unless this regulatory guide is part of the licensing basis for a facility, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this regulatory guide constitutes a violation.

---

[3] In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and the term "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52, and applicants for standard design approvals and standard design certifications under 10 CFR Part 52.

[4] In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

If an existing licensee voluntarily seeks a license amendment or change and: (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised regulatory guide and (2) the specific subject matter of this regulatory guide is an essential consideration in the staff's determination of the acceptability of the licensee's request, then the NRC staff may request that the licensee either follow the guidance in this regulatory guide or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

Additionally, an existing applicant may be required to comply with new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

If a licensee believes that the NRC is either using this regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 29) and NUREG-1409, "Backfitting Guidelines," (Ref. 23).

REFERENCES[5]

1. *U.S. Code of Federal Regulations* (CFR), "Physical Protection of Plants and Materials," Part 73, Chapter I, Title 10, "Energy."

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

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

4. CFR, "Licensing Requirements for Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor Related Greater than Class C Waste," Part 72, Chapter I, Title 10, "Energy."

5. NRC, Regulatory Guide (RG) 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition), Washington, DC.

6. NRC, RG 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials, Classified Matter, and Safeguards Information," Washington, DC.

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

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

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

10. NRC, RG 5.69, "Guidance for the Application of the Radiological Design Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," Washington, DC.

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.

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

---

[5] 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 online 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.

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

17. NRC, RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors," Washington, DC.

18. NRC NUREG-0908, "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans."

19. Nuclear Energy Institute (NEI), NEI 03-12, Revision 7, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]."[6]

20. IAEA, Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/255/Revision 5), IAEA, Vienna, Austria, 2011.[7]

21. NRC, NUREG/CR-6190, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants," Washington, DC.

22. PDC-TR 06-05, Rev.1, "Evaluating Adequacy of Landform Obstacles as Vehicle Barriers," U.S. Army Corps Of Engineers, Washington, DC, August 2007.[8]

23. NRC, NUREG/CR-4250, "Vehicle Barriers: Emphasis on Natural Features," U.S. Nuclear Regulatory Commission, Washington, DC.

24. United States Army Field Manual, FM 3-19.30, "Physical Security," U.S. Army Corps Of Engineers, Washington, DC, Janaury 8, 2001.

25. PDC-TR 06-03, "Vehicle Barrier Maintenance Guidance," U.S. Army Corps Of Engineers, Washington, DC, February 2007.

26. NRC, Security Advisory 06-04, "Implementing Search Requirements and Approved Exceptions for Packages and Materials at NRC-Licensed Facilities," Washington, DC. (Not Publicly Available: Secure Agency-Wide Database for Safeguards Information (eSAFE) Accession Number: NS103607).

---

[6] Publications from the Nuclear Energy Institute (NEI) are available at their Web site: http://www.nei.org/ or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street NW, Washington DC 20006-3708, Phone: 202-739-800, Fax 202-785-4019.

[7] 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

[8] Copies of U.S. Army Corps of Engineers documents may be obtained from the Corps at: Headquarters, U.S. Army Corps of Engineers, 441 G Street, NW, Washington, DC 20314-1000, or electronically from their web site: http://publications.usace.army.mil/publications/

27. NRC, SFAQ 10-03, "Verification of Bulk or Hazardous Materials," Washington, DC. (Not Publicly Available: Agencywide Documents Access and Management System (ADAMS) Accession No. ML102290452).

28. NRC, Information Notice No. 96-71, "Licensee Response to Indications of Tampering, Vandalism, or Malicious Mischief," Washington, DC.

29. NRC, Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," U.S. Nuclear Regulatory Commission, Washington, DC.

30. NRC, NUREG-1409, "Backfitting Guidelines," Washington, DC.

BIBLIOGRAPHY

Information Notices

NRC Information Notice 89-05, "Use of Deadly Force by Guards Protecting Nuclear Power Reactors Against Radiological Sabotage," U.S. Nuclear Regulatory Commission, Washington, DC.

Miscellaneous NSIR Documents[9]

NSIR/STD-2004/15-001, "Composite Adversary Force Performance Standards for Force-on-Force Exercises," Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, May 2005.

SFAQ 05-10, "Tactical Qualification Course of Fire."

SFAQ 10-02, "Qualification of Armed Responders during Security Drills."

SFAQ 10-13, "Security Shift Supervisor."

SFAQ 12-03, "NEI 03-12, Revision 7 – Hostage Training & Qualification."

SFAQ 12-04, "NEI 03-12, Revision 7 – Watchperson Definition, Duty Position & Task Matrix."

SFAQ 12-07, "NEI 03-12, Revision 7 – Insider Mitigation (two-person)."

SFAQ 12-11, "OCA Vehicle Search/Escort."

SFAQ 12-08, "Vehicle Search at Checkpoint."

SFAQ 12-05, "NEI 03-12, Revision 7 – Contingency Event #21."

[9] The documents listed as miscellaneous are not publicly available.