U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

13.6.1 PHYSICAL SECURITY—COMBINED LICENSE AND OPERATING REACTORS

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of physical security

Secondary - None

I. AREAS OF REVIEW

The review evaluates the security plans (physical security, training and qualification, and safeguards contingency plans collectively, the Security Plan), which together describe a comprehensive physical security program for combined license (COL) applicants and operating reactor licensees. The review encompasses the regulatory requirements in Title 10 of the *Code of Federal Regulations* (CFR), Section 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," and Appendix B, "General Criteria for Security Personnel," and Appendix C, "Nuclear Power Plant Safeguards Contingency Plans," to 10 CFR Part 73, "Physical Protection of Plants and Materials." It includes the physical security organization; access controls, including physical barriers; searches of personnel, materials, and vehicles; a means of detection, assessment, delay, and response; the selection of personnel for security purposes; training and qualifying security personnel; the response to contingency events; and arrangements with law enforcement authorities for assistance in responding to security threats. It also includes a review of the

USNRC STANDARD REVIEW PLAN

This Standard Review Plan (SRP), NUREG 0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission (NRC) staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The SRP sections are numbered in accordance with corresponding sections in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of Regulatory Guide 1.70 have a corresponding review plan section. The SRP sections applicable to a COL application for a new light-water reactor (LWR) are based on Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG 0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted electronically by e-mail to NRR_SRP@nrc.gov.

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section, by fax to (301) 415 2289; or by e-mail to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC's public Web site at http://www.nrc.gov/reading rm/doc collections/nuregs/staff/sr0800/, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading rm/adams.html, under Accession No. ML100350158.

description for implementation of the security plan (implementation schedule) for the physical security program, including phases for a multiunit plant, where applicable.

In addition to the requirements outlined in 10 CFR 73.55 and Appendices B and C to 10 CFR Part 73, the Security Plan must describe measures that will be taken to meet the general performance objective of 10 CFR 73.55(b) to ensure, by implementing the requirements in 10 CFR 73.55(a) through (k), that the overall level of system performance provides high assurance of the protection against the design-basis threat (DBT) of radiological sabotage, as defined in 10 CFR 73.1, "Purpose and Scope."

The staff of the U.S. Nuclear Regulatory Commission (NRC) may review the Security Plan for correct format and content, using the most recent NRC-endorsed revision of Nuclear Energy Institute (NEI) 03-12, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Security Program]." If the NRC staff identifies any deviations from the template in the Security Plan, it will review them using the attached appendices and the review procedures outlined in this SRP.

For COL applications, the NRC staff must also review the inspections, tests, analyses, and acceptance criteria (ITAAC) and COL action or information items that are relevant to this Standard Review Plan (SRP) section. Physical security hardware ITAAC and the corresponding review procedures relevant to this section are in SRP Section 14.3.12, "Physical Security Hardware—Inspections, Tests, Analyses, and Acceptance Criteria (PS-ITAAC)."

Additional considerations in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," are listed below.

1. For a COL application referencing a design certification (DC), the applicant must address COL items (referred to as COL license information items in certain DCs) included in the referenced DC. Additionally, a COL applicant must address requirements and restrictions (e.g., interface requirements and site parameters) included in the referenced DC. COL applicants referencing an early site permit (ESP) must address ESP COL items in the COL application.

2. For a COL application, the staff reviews the security plans which describe the weapons training, qualification, and requalification programs; the physical security program; the performance evaluation program; the insider mitigation program; the access authorization program; the fitness-for-duty (FFD) program description; vehicle control measures; and the proposed implementation milestones. The staff also reviews Table 13.4 in the final safety analysis report (FSAR) to ensure that it includes the milestones associated with these programs.

3. The staff reviews the FSAR description of the physical security program, Section 13.6.

4. Regulations in 10 CFR 52.17(a)(1)(x) state that an applicant will provide information to demonstrate that its site characteristics are such that adequate security plans and measures can be developed.

5. COL applicants that address a limited work authorization must address, in the COL application, the requirements of 10 CFR Part 26, "Fitness for Duty Programs," Subpart

K, “FFD Programs for Construction,” during new reactor construction. SRP Section 13.7, “Fitness for Duty (FFD),” addresses FFD requirements.

Review Interfaces

Other SRP sections interface with this section as follows:

1. For COL reviews of operational programs, the reviewer uses the applicant’s description of its implementation of security plans (implementation schedule) under SRP Section 13.4, “Operational Programs.”

2. The reviewer uses SRP Section 14.3.12 to determine the adequacy of the PS-ITAAC.

The referenced SRP sections contain the specific acceptance criteria and review procedures.

II. ACCEPTANCE CRITERIA

Requirements

The NRC bases its acceptance criteria on the relevant requirements of the following regulations:

1. 10 CFR Part 26, “Fitness for Duty Programs”

2. 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities”

3. 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants”

4. 10 CFR 73.1, “Purpose and Scope”

5. 10 CFR 73.2, “Definitions”

6. 10 CFR 73.21, 10 CFR 73.22, and 10 CFR 73.23, “Protection of Safeguards Information”

7. 10 CFR 73.55, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage”

8. 10 CFR 73.56, “Personnel Access Authorization Requirements for Nuclear Power Plants”

9. 10 CFR 73.57, “Requirements for Criminal History Checks of Individuals granted Unescorted access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees”

10. 10 CFR 73.58, “Safety/Security Interface Requirements for Nuclear Power Reactors”

11. 10 CFR 73.70, “Records”

12. 10 CFR Part 73, Appendix B VI, “Nuclear Power Reactor Training and Qualification Plan for Security Personnel Performing Security Program Duties”

13. 10 CFR Part 73, Appendix C II, “Nuclear Power Plant Safeguards Contingency Plans”

SRP Acceptance Criteria

Specific SRP acceptance criteria that meet the relevant requirements of the above regulations are as follows for the review described in this SRP section. The SRP is not a substitute for the NRC’s regulations, and compliance with it is not required. However, the NRC requires an applicant or an operating reactor licensee to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and to evaluate how the proposed alternatives to the SRP acceptance criteria provide acceptable methods of compliance with the NRC regulations.

The Security Plan is considered acceptable if it conforms to the most recent revision of the NRC-endorsed NEI 03-12 format and the requirements listed in Appendices I, II, and III of this document.

The NRC considers that the site-specific information in the most recent revision of the NRC-endorsed NEI 03-12 generic security plan template (site-specific bracketed text) describes a physical security program that meets the level of detail required for submitted security plans.

1. The physical security plan describes the physical protection program that provides high assurance against the DBT outlined in 10 CFR 73.1(a) to ensure that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety (Appendix I).

    A. 10 CFR 73.21, 10 CFR 73.22, and 10 CFR 73.23—Protection of Safeguards Information. These regulations establish the requirements for the protection of Safeguards Information (SGI). Compliance with these sections provides assurance that SGI is protected against unauthorized disclosure.

    B. Section (d) of 10 CFR 73.55—Physical Security Organization. The licensee shall establish a security organization, including security officers, to protect the facility against radiological sabotage. These general criteria establish requirements for selecting, training, equipping, testing, and qualifying individuals who will be responsible for protecting special nuclear materials, nuclear facilities, and nuclear shipments.

    C. Section (e) of 10 CFR 73.55—Physical Barriers. The licensee shall locate vital equipment only within vital areas, which must be located within a protected area, so that access to vital equipment requires passage through at least two physical barriers, as defined in 10 CFR 73.2. The licensee shall also provide isolation zones adjacent to the protected area perimeter barrier and shall monitor them in accordance with 10 CFR 73.55(e)(7)(i)(B) and (C) The reactor control room, the central alarm station, the location within which the last access control function for

access to the protected area is performed, and (in accordance with 10 CFR 73.55(i)(4)(iii)) the secondary alarm station must be bullet-resisting. The licensee shall establish vehicle control measures in accordance with the requirements of 10 CFR 73.55(e)(10).

D. Section (f) of 10 CFR 73.55—Target Sets. 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 target set equipment and elements. The licensee shall consider cyber attacks in the development and identification of target sets. Target set equipment or elements that are not within a protected or vital area must be identified and documented and accounted for in the licensee's protective strategy. The licensee shall implement a process for the oversight of target set equipment and systems to ensure that changes to configuration of the identified equipment or systems are considered in the licensee's protective strategy and where appropriate, changes must be made to documented target sets.

E. Section (g) of 10 CFR 73.55—Access Controls. Consistent with the function of each barrier or barrier system, the licensee shall control personnel, vehicle, and material accesses, as applicable, at each access control point. The licensee shall design access authorization and access control systems to accommodate the rapid entry and exit of authorized individuals and vehicles during emergency conditions or in situations that could lead to emergency conditions. The access authorization and access control systems shall ensure that vital area access is controlled during nonemergency conditions by locking and alarming unoccupied vital areas consistent with 10 CFR 73.55(e)(9)(iii). The licensee shall control all keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems. In accordance with 10 CFR 73.70(d), records shall document the vital area entry and exit of individuals.

F. Section (h) of 10 CFR 73.55—Search Requirements. Each 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.

G. Section (i) of 10 CFR 73.55—Detection and Assessment Systems. Intrusion detection equipment must annunciate, and video assessment equipment must display, concurrently in at least two continuously staffed onsite alarm stations that are designed and equipped to ensure that a single act, in accordance with the DBT of radiological sabotage cannot disable both alarm stations. The central alarm station must be located inside the protected area and must be: considered a vital area in accordance with 10 CFR 73.55(e)(9)(v)(C) ; bullet-resisting consistent with 10 CFR 73.55(e)(5); configured so the interior is not be visible from the protected area perimeter. Applicants for a license under 10 CFR Part 50 or 10 CFR Part 52 shall construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station. Intrusion detection and assessment equipment at the protected area perimeter must remain operable from an uninterruptible power supply.

Consistent with 10 CFR 73.55(e)(9)(iii), all associated onsite secondary power supplies for alarm annunciators and non-portable communications equipment must be located within vital areas. All emergency exits from protected and vital areas must be locked and alarmed consistent with 10 CFR 73.55(e)(9)(ii).

H. Section (j) of 10 CFR 73.55—Communications Requirements. All on-duty security force personnel (watchman, armed security officer, armed responder, or other designated security personnel performing security functions in support of the physical protection program and protective strategy) shall be capable of maintaining continuous communications with an individual in each alarm station. Vehicle escorts shall be able to maintain continuous communications with security personnel. The licensee shall establish conventional telephone and radio or microwave-transmitted two-way voice communications with local law enforcement authorities.

I. Section (k) of 10 CFR 73.55—Response Requirements. Consistent with Appendix C II to 10 CFR Part 73, the licensee shall establish, maintain, and follow an NRC-approved safeguards contingency plan. The licensee shall maintain liaison with local law enforcement authorities. Each licensee shall maintain an adequate number of armed personnel for response to and assessment of possible security threats. Each licensee shall require the security organization to evaluate and neutralize the threat, when detected, with sufficient force to counter the force of the threat.

J. Section (m) of 10 CFR 73.55—Security Program Reviews. As a minimum, the licensee shall review each element of the physical protection program at least every 24 months. Reviews of the security program must include an audit of the effectiveness of the physical security program; security plans; implementing procedures; cyber security program; safety and security interface activities; testing, maintenance, and calibration programs; and response commitments by local, State, and Federal law enforcement authorities.

K. Section (n) of 10 CFR 73.55—Maintenance, Testing, and Calibration. Each licensee shall establish, maintain, and implement a maintenance, testing, and calibration program, to ensure that it tests security systems and equipment, including secondary and uninterruptible power supplies, for operability and performance at predetermined intervals, maintains them in an operable condition, and ensures they are capable of performing their intended function.

L. Section (o) of 10 CFR 73.55—Compensatory Measures. The licensee shall identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components. Compensatory measures must provide a level of protection that is equivalent to that which the degraded or inoperable equipment, system, or component provided.

M. Section (p) of 10 CFR 73.55—Suspension of Security Measures. Licensees shall ensure that the criterion and requirements for suspending security measures identified within this paragraph of the regulation are followed.

N. Section (q) of 10 CFR 73.55—Records. The licensee shall maintain all records required to be kept by Commission regulations, orders, or licensing conditions, until the Commission terminates the license for which the records were developed and it shall maintain superseded portions of these records for at least 3 years after the record was superseded, unless otherwise specified by the Commission.

O. 10 CFR 52.47(b)(1)—DC ITAAC. A DC application must contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the DC has been constructed and will be operated in conformity with the DC, the provisions of the Atomic Energy Act (AEA), and the NRC's regulations.

P. 10 CFR 52.80(a)—COL ITAAC. A COL application must contain the proposed inspections, tests, and analyses, including those applicable to emergency planning, that the licensee shall perform, and the acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, the facility has been constructed and will operate in conformity with the COL, the provisions of the AEA, and the NRC's regulations.

2. The training and qualification plan (Appendix B to a security plan) provides the general criteria for security personnel, which, in accordance with Appendix B VI to 10 CFR Part 73, establishes requirements for selecting, training, equipping, testing, and qualifying individuals who are responsible for the protection of special nuclear materials, nuclear facilities, and nuclear shipments, and personnel who perform security duties (Appendix II).

3. The safeguards contingency plan (Appendix C of a security plan), in accordance with Appendix C II to 10 CFR Part 73, establishes defined objectives in the event of threats, thefts, or radiological sabotage relating to special nuclear material or nuclear facilities. The plan contains: (1) Background-an overview of the plan's purpose and goals, (2) Generic Planning Base-the identification of initiation conditions, with objectives to be accomplished for each condition, and the identification of the data, criteria, procedures, and mechanisms necessary to efficiently implement decisions, (3) Licensee Planning Base-a description of the site-specific design, organizational structure for response, security systems, and defense in depth (protective strategy), (4) Responsibility Matrix-the identification of a mechanism that describes individuals, groups, or organizational entities responsible for each decision and action, and (5) Implementing Procedures-a description of implementing procedures (Appendix III).

4. For COL applications, the NRC reviews the description of the operational program and the proposed implementation milestone(s) for the physical security program, in accordance with 10 CFR 73.55; for the security training and qualification program, in accordance with 10 CFR Part 73, Appendix B, Section VI, A through I; for the safeguards contingency response program, in accordance with 10 CFR Part 73, Appendix C, Section II; for the access authorization program, in accordance with 10 CFR 73.56; for the FFD program, in accordance with 10 CFR

Part 26. The implementation milestone for the completion of all operational programs in this section is before fuel is allowed onsite (protected area).

Technical Rationale

The following paragraphs contain the technical rationale for applying these acceptance criteria to the areas of review addressed by this SRP section:

1. 10 CFR Part 26 establishes the requirements for FFD programs to ensure that licensee personnel are not under the influence of the substances identified in 10 CFR Part 26, or impaired from fatigue under 10 CFR Part 26, Subpart I, that may adversely affect their ability to safely and competently perform their duties. SRP Section 13.7 addresses the FFD requirements of 10 CFR Part 26.

2. 10 CFR 50.34(c)(2) and 10 CFR 73.55(c)(3) require a physical security plan that describes how the applicants will meet the requirements of 10 CFR Part 73 and 10 CFR Part 11, "Criteria and Procedures for Determining Eligibility for Access to or Control over Special Nuclear Material," if applicable (see Appendix I). See the technical rationale for 10 CFR 73.55 (Item 11) below.

3. 10 CFR 50.34(c)(2) and 10 CFR 73.55(c)(4) require applicants for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55 to include a training and qualification plan in accordance with the criteria set forth in 10 CFR Part 73, Appendix B VI (see Appendix II). See the technical rationale for Appendix B VI to 10 CFR Part 73 (Item 14) below.

4. 10 CFR 50.34(d)(2) and 10 CFR 73.55(c)(5) require applicants for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55 to include a safeguards contingency plan in accordance with the criteria set forth in 10 CFRPart 73, Appendix C, Section II (see Appendix III). See the technical rationale for Appendix C II to 10 CFR Part 73 (Item 15) below.

5. 10 CFR 50.54(p)(1) requires the licensee to prepare and maintain procedures consistent with the safeguards contingency plan for effecting the actions and decisions of the responsible organizations, as described in the plan. This SRP section reviews the safeguards contingency plan. Compliance with 10 CFR 50.54(p) provides assurance that procedures are developed to provide a structured, disciplined, and organized approach to executing the safeguards contingency plan in response to perceived dangers to the facility, personnel, or special nuclear material, as described in the plan.

6. 10 CFR 52.79(a)(35)(i), which requires each applicant for a combined license (COL) for a utilization facility that will be subject to the requirements of 10 CFR 73.55, Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," to include a physical security plan.

7. 10 CFR 52.79(a)(36)(i), which requires each applicant for a license to operate a utilization facility that will be subject to 10 CFR 73.55, to include a licensee safeguards contingency plan in accordance with the criteria set forth in Section II of Appendix C, "Nuclear Power Plant Safeguards Contingency Plans," to 10 CFR Part 73.

8. 10 CFR 52.79(a)(36)(ii), which requires each applicant for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55, to include a training and qualification plan in accordance with the criteria set forth in Appendix B VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," to 10 CFR Part 73, "Physical Protection of Plants and Materials."

9. 10 CFR 52.79(a)(36)(iii), which requires each applicant for a license to operate a utilization facility that will be subject to the requirements of 10 CFR 73.55, to include a and a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."

10. 10 CFR 73.21, 10 CFR 73.22, and 10 CFR 73.23 establish the requirements for the protection of SGI, which includes the physical security plan, safeguards contingency plan, and any elements of the training and qualification plan that disclose information related to the physical security system or response procedures. The unauthorized disclosure of this information could compromise the ability of the security organization to provide an appropriate level of protection against, and response to, threats, theft, and radiological sabotage.

11. 10 CFR 73.55 establishes the detailed requirements for the development and implementation of a physical protection program, which includes the administrative, physical, and operational measures that provide protection of the facility, and any associated special nuclear material, from both internal and external threats. Compliance with 10 CFR 73.55 (see Appendix I) provides high assurance that a facility is protected against the DBT of radiological sabotage.

12. 10 CFR 73.56 establishes the requirements for the development and implementation of an access authorization program, as part of the physical security plan, for granting individuals unescorted access to protected and vital areas. The physical security plan contains a program description of the access authorization program that is reviewed under this SRP section. Compliance with 10 CFR 73.56 provides assurance that individuals granted unescorted access are trustworthy and reliable and do not constitute an unreasonable risk to the public health and safety, including a potential to commit radiological sabotage.

13. 10 CFR 73.57 establishes the requirements for performing criminal history checks of individuals granted unescorted access to a nuclear power facility or Safeguards Information. This SRP section reviews access authorization as part of the physical security plan.

14. 10 CFR Part 73, Appendix B VI, establishes the requirements for selecting, training, qualifying, and equipping security personnel responsible for protecting nuclear facilities against the DBT of radiological sabotage (see Appendix II). Security personnel qualified in accordance with Appendix B are an integral part of the physical security plan required by 10 CFR 73.55 and are reviewed under this SRP section. Compliance with the requirements of Appendix B VI to 10 CFR Part 73 provides assurance that security

personnel are adequately prepared to identify, respond to, and repel threats to the nuclear facility and material.

15. 10 CFR Part 73, Appendix C II, establishes the requirements for a safeguards contingency plan (see Appendix III). The safeguards contingency plan is a documented plan to provide guidance to licensee personnel responding to threats, thefts, or radiological sabotage relating to nuclear facilities. The safeguards contingency plan is an integral part of the response capabilities and requirements of the physical security plan developed in accordance with 10 CFR 73.55 and reviewed under this SRP section. Compliance with Appendix C II to 10 CFR Part 73 provides assurance that a licensee is adequately prepared to respond to perceived dangers of nuclear material theft or radiological sabotage.

III. REVIEW PROCEDURES

The scope of the review of a COL application is dependent on whether the COL applicant references a DC, an ESP, a limited work authorization, or other NRC approvals (e.g., manufacturing license, site suitability report, or topical report). The reviewer should then review Tier I information for the design, including the postulated site parameters, interface criteria, and ITAAC.

The reviewer will select material from the procedures described below, as may be appropriate for a particular case. The reviewer verifies that the licensee's security program is fully described in the physical security plan, training and qualification plan, and safeguards contingency plan and, for COL applicants, that implementation milestones have been identified.

For COL applicants, implementation of physical security programs will be inspected in accordance with NRC inspection Manual Chapter IMC-2504 "Construction Inspection Program - Inspection of Construction and Operational Programs."

For operating reactor licensees, implementation of physical security programs will be inspected in accordance with NRC Inspection Manual Chapter IMC-2201 "Security Inspection Program for Commercial Nuclear Power Reactors."

The identified SRP acceptance criteria form the basis for these review procedures. For deviations from these acceptance criteria (such as alternative measures, in accordance with 10 CFR 73.55(r)), the staff should review the applicant's or licensee's submittal under 10 CFR 73.55(r) which would be submitted in accordance with 10 CFR 50.4 and 10 CFR 50.90 and should describe how the proposed alternatives provide an acceptable method of complying with the relevant NRC requirements identified in this section of the SRP and in Section II above.

When conducting the review of security plans the reviewer should determine whether the Security Plan conforms to the most recent NRC-endorsed revision of the generic security plan, NEI 03-12 (template), regulations, and the information requirements of Section I above and the acceptance criteria of Section II above.

Site-specific information should be reviewed and evaluated in accordance with the requirements of 10 CFR Part 73, endorsed NEI 03-12 (template), any NRC approved alternative measure the

licensee has submitted in accordance with 10 CFR 73.55(r), and the review procedures identified below.

Physical Security Plan

Introduction: 10 CFR 73.55(a)

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.

Licensees are responsible for maintaining the onsite physical protection program in accordance with Commission regulations through the implementation of security plans and written security implementing procedures.

Applicants for an operating license under the provisions of 10 CFR Part 50 or holders of a COL under the provisions of 10 CFR Part 52 shall implement the requirements of 10 CFR 73.55 before fuel is allowed on site (protected area). Regulatory Guide (RG) 5.76, "Physical Protection Programs at Nuclear Power Reactors," contains additional guidance concerning this requirement.

Applicants for an operating license under the provisions of 10 CFR Part 50 or holders of a COL under the provisions of 10 CFR Part 52 that do not reference a standard DC or that reference a standard DC issued after May 26, 2009, shall meet the requirement of 10 CFR 73.55(i)(4)(iii).

General Performance Objectives and Requirements: 10 CFR 73.55(b)

The 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.

The physical protection program must protect against the DBT, as stated in 10 CFR 73.1.

The physical protection program must be designed to prevent significant core damage and spent fuel sabotage. Specifically, the program must do the following:

- Ensure that the ability to detect, assess, interdict, and neutralize threats, up to and including the DBT of radiological sabotage, as stated in 10 CFR 73.1, is maintained at all times.

- Provide defense in depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures, as needed, to ensure the effectiveness of the physical protection program.

The licensee shall analyze and identify site-specific conditions, including target sets, that may affect the specific measures needed to implement the requirements of this section and shall account for these conditions in the design of the physical protection program.

Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability to meet Commission requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

The licensee shall establish, maintain, and implement a performance evaluation program, in accordance with Appendix B VI to 10 CFR Part 73, to demonstrate and assess the effectiveness of armed responders and armed security officers to implement the licensee's protective strategy.

The licensee shall establish, maintain, and implement an access authorization program in accordance with 10 CFR 73.56 and shall describe the program in the physical security plan.

The licensee shall establish, maintain, and implement a cyber security program in accordance with 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."

The licensee shall establish, maintain, and implement an insider mitigation program and shall describe the program in the physical security plan.

The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's ability to prevent significant core damage and spent fuel sabotage.

The insider mitigation program must contain elements from the following:

- the access authorization program described in 10 CFR 73.56
- the FFD program described in 10 CFR Part 26
- the cyber security program described in 10 CFR 73.54
- the physical protection program described in 10 CFR 73.55

The licensee shall use the site corrective action program to track, trend, correct, and prevent the recurrence of failures and deficiencies in the physical protection program.

The licensee must coordinate the implementation of security plans and associated procedures with other onsite plans and procedures to preclude conflict under both normal and emergency conditions.

Guidelines

The physical security plan shall describe the programs, systems, and measures that the licensee implements to support the overall physical protection of the site and confirm that they meet the general performance objective and requirements of 10 CFR 73.55.

The licensee shall design and maintain the physical protection system to ensure the protection of special nuclear material.

Key physical protection system elements should include security personnel, detection and assessment systems, physical security barriers, access controls, search programs, cyber security, information security, personnel security, and contingency plans.

The physical security plan fully describes the access authorization program, in accordance with 10 CFR 73.56, although a full description is not necessary when the plan confirms that the licensee has used the most current revision of RG 5.66, "Access Authorization Program for Nuclear Power Plants." RG 5.66 provides acceptable language for insertion into site security plans to describe the access authorization program.

The physical security plan fully describes the insider mitigation program, in accordance with 10 CFR 73.55 and 10 CFR 73.56, although a full description is not necessary when the plan confirms that the licensee has used the most current revision of RG 5.77, "Insider Mitigation Program."

Security Organization: 10 CFR 73.55(d)

Guidelines

The physical security plan shall describe the security organization, which should, at a minimum, include the following positions: security manager, access authorization supervisor or access authorization/FFD supervisor, security shift supervisor, armed response team leader, armed responders, armed security officers, alarm station operators, watchpersons, and security instructors.

An acceptable physical security plan would identify the positions within the security organization, with a position description for each.

An acceptable physical security plan would confirm that the security organization does not have any other responsibilities that would conflict with its responsibility to protect against radiological sabotage.

The physical security plan shall confirm that the security organization is designed, staffed, trained, qualified, and equipped to implement the physical protection program, including the protective strategy.

The physical security plan should describe the management system that provides oversight of the onsite physical protection program, the purpose of which is to develop, revise, implement, and oversee security procedures.

The physical security plan should describe how written approvals of procedures and revisions by the individual with overall responsibility for the site security program (security director or manager) are a part of the management system.

The physical security plan should describe, by position title, the individual who is on site at all times who has the authority to direct the activities of the security organization. This individual

should not be assigned any other duties that would interfere with the ability to perform the assigned duties.

A physical security plan that describes the use of non-security personnel should confirm that these individuals are properly equipped to perform assigned duties and that they possess the knowledge, skills, and abilities, including physical attributes (sight and hearing), to perform their assigned duties and responsibilities.

If contractors are used, the physical security plan should describe the use of such individuals and ensure that these individuals are trained and qualified to perform the functions that they are assigned in the security organization.

The security plan must state that the contract is retained as a record.

Physical Barriers: 10 CFR 73.55(e)

Guidelines

A typical physical security plan would confirm that access to the protected area is controlled through physical barriers. The security plan would also describe the use of physical barriers in the owner-controlled area, protected area, and vital areas.

A physical security plan shall confirm that the reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed must be bullet-resisting. For COL applicants, this would include the secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii).

The physical security plan shall describe bullet-resisting physical barriers for the reactor control room; central alarm station; bullet-resisting protected positions; the location within which the last access control function for access to the protected area is performed; and, for COL applicants, the secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii). An acceptable physical security plan would typically define "bullet resistant" as having a minimum capability of resisting a high-powered rifle round, as identified in Regulatory Guide 5.76 "Physical Protection Programs at Nuclear Power Reactors," paragraph 4.6.

Physical security plans shall describe the use of barriers in the owner-controlled area, protected area, and at vital areas to implement the site physical protection program, including the type of barriers used (e.g., buildings, topography, fences, walls, doors, etc.).

Isolation Zones: 10 CFR 73.55(e)(7)

Guidelines

Physical security plans shall describe the location of isolation zones and areas of the protected area perimeter where isolation zones are not maintained because of site specific characteristics, as identified in 10 CFR 73.55(e)(8)(iv).

The description of isolation zones in the security plan shall confirm that these zones are monitored with intrusion detection equipment that is capable of detecting attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier and is monitored with assessment equipment capable of providing real-time and playback/recorded video images of detected activity before and after each alarm annunciation.

Protected Area: 10 CFR 73.55(e)(8)

Guidelines

The descriptions of the protected area barrier provided in the physical security plan must meet the criterion established for physical barriers in 10 CFR 73.2.

The physical security plan shall describe the extent to which the protected area barrier at the perimeter is separated from vital area barriers. The physical security plan shall also describe areas where building walls or roofs comprise a portion of the protected area perimeter barrier and where isolation zones are not maintained. This description should address the intrusion detection and assessment capabilities and physical barriers that protect these areas, to meet the requirements of 10 CFR 73.55.

The description of the protected area barrier shall also address the protection provided against penetrations of the barrier, including unattended openings that intersect a security boundary, such as underground pathways. The description of these areas shall confirm that they are protected, as required by 10 CFR 73.55(e)(8)(ii) and 10 CFR 73.55(i)(5)(iii).

Vital Areas: 10 CFR 73.55(e)(9)

Guidelines

The physical security plan shall describe a vital area as an area that contains vital equipment.

The physical security plan shall confirm that access to vital equipment requires passage through at least two physical barriers and that each barrier meets the criterion established for physical barriers in 10 CFR 73.2.

The physical security plan shall confirm that all points of personnel and vehicle access into a vital area are positively controlled and that these points are locked and alarmed.

The security plan shall describe the areas that the licensee has designated as vital areas, which, at a minimum, shall include the reactor control room; the spent fuel pool; the central alarm station; and, for COL applicants, the secondary alarm station, in accordance with 10 CFR 73.55(i)(4)(iii).

Vehicle Control Measures (Vehicle Barriers): 10 CFR 73.55(e)(10)

Guidelines

The physical security plan shall contain a description of the vehicle barriers and their use and placement. A site drawing shall depict the location of the vehicle barrier system, including active and passive barriers.

The description should provide detailed information regarding the facility's use of vehicle barriers to meet the requirements of 10 CFR 73.55 for protection against the DBT vehicle bomb,

as described in 10 CFR 73.1. RG 5.69 “Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program That Meets 10 CFR 73.55 Requirements” contains additional details of the characteristics for the design-basis vehicle threat.

Each physical security plan shall confirm that periodic checks for the operability of active vehicle barrier systems are performed in accordance with facility procedures.

The physical security plan shall describe the periodic surveillance and observation of vehicle barrier systems to detect indications of tampering and degradation and to ensure the system meets its intended function.

The physical security plan shall describe the protective measures for rail access to the protected area and confirm that periodic surveillance of the protective measures is implemented. The physical security plan shall describe the surveillance methods implemented for the protective measures at rail access points.

Target Sets: 10 CFR 73.55(f)

Guidelines

The physical security plan shall describe the process the licensee has established and implemented to develop and identify target sets.

The physical security plan will confirm that cyber attacks were considered during the development and identification of target sets.

The physical security plan shall confirm that the licensee’s protective strategy accounts for target set equipment not within a protected or vital area.

The physical security plan shall describe or confirm that a process exists for the oversight of target set equipment and systems to include configuration changes that could change the licensee’s protective strategy and provides details in the implementing procedures. The physical security plan should also confirm that where appropriate, changes to targets sets shall be documented.

Access Controls: 10 CFR 73.55(g)

Guidelines

The physical security plan describes access control points and the measures implemented to restrict access to authorized personnel only. The description should identify the location of the access control points for personnel, material, and vehicle access to the site protected area.

The physical security plan shall confirm that access portals are equipped with locking devices, intrusion detection equipment, and surveillance equipment, consistent with the function of the access point.

The physical security plan shall describe the process to provide supervision and control to the badging process to prevent unauthorized bypass of the access control equipment located at or outside of the protected area.

An acceptable physical security plan would identify the individuals or post responsible for the last access control function to the protected area, describe their duties to control admission to the protected area, and explain whether they provide response or summon assistance during security events.

Vehicle Control Measures: 10 CFR 73.55(g)(1)

Guidelines

An acceptable physical security plan would describe the controls (consistent with the intended function of the barrier) implemented at vehicle barrier portals (owner-controlled area, protected area, vital area) to ensure that only authorized vehicles are granted access through the barrier.

The physical security plan should describe how search functions (protected area and if applicable owner-controlled area) are observed to ensure that a response can be initiated in accordance with 10 CFR 73.55(h).

Physical layout diagrams that are part of the security plan should depict the location of access control points through vehicle barrier systems.

Protected Area Access: 10 CFR 73.55(g)(2)

Guidelines

The physical security plan shall describe the process to confirm the identity of individuals.

The physical security plan shall confirm that authorization for protected area access is verified for individuals, vehicles, and materials before entry into the protected area.

An acceptable physical security plan shall confirm that personnel entering the protected area are not currently denied access to another licensed facility.

The physical security plan shall confirm that all personnel, material, and vehicles are subjected to the search process, as required by 10 CFR 73.55(h), before they enter the protected area.

Physical layout diagrams that are part of the security plan should depict the location of the protected area barrier and the access control points through the barrier.

Vehicle Access into Protected Area: 10 CFR 73.55(g)(3)

Guidelines

An acceptable physical security plan would confirm that vehicles in the protected area are operated only by personnel who possess unescorted access and have been authorized to use the vehicle for authorized purposes in support of plant functions or emergency conditions. Keys must be removed or the vehicle otherwise disabled when not in use.

The physical security plan shall confirm that personnel who do not possess unescorted access and who operate vehicles within the protected area are escorted, as required by 10 CFR 73.55(g)(8).

The physical security plan shall confirm that vehicles transporting hazardous materials inside the protected area are escorted by an armed member of the security organization.

Vital Area Access: 10 CFR 73.55(g)(4)

Guidelines

The physical security plan shall confirm that access to vital areas during nonemergency conditions is limited to individuals who require access to perform their duties consistent with 10 CFR 73.55(g)(1)(i)(D). The plan shall also confirm that access to vital areas is controlled consistent with vital area access authorization lists.

The physical security plan shall confirm that the licensee has a process to review access authorization lists (in accordance with 10 CFR 73.56(j) at a frequency no less frequently than every 31 days) to assess the continued need of individuals to access specific vital areas to perform duties and responsibilities.

Emergency Conditions: 10 CFR 73.55(g)(5)

Guidelines

The physical security plan shall describe how the design of the access control system accommodates the need for rapid entry or exit of authorized individuals during emergency conditions or situations.

The physical security plan shall confirm that security implementing procedures are in place for emergency conditions to ensure prompt access to authorized emergency personnel for affected areas and equipment.

Access Control Devices: 10 CFR 73.55(g)(6)

Guidelines

The physical security plan shall describe how all security keys, locks, combinations, passwords, and related access control devices used to access protected areas, vital areas, and security systems are controlled to reduce the probability of compromise.

An acceptable physical security plan would confirm that access control devices to protected areas, vital areas, and security systems are distributed only to those individuals who have unescorted access and require access to perform official duties and responsibilities.

The physical security plan shall describe how compensatory measures are implemented when the licensee suspects that access control devices have been compromised or when it has terminated an individual with access to such devices under less than favorable conditions. The description should also include a timeframe for implementing compensatory measures for conditions that could degrade the security program.

A physical security plan should state whether access authorization program personnel are given passwords, combinations, or other access control devices. The plan shall confirm that personnel who are given access control devices meet the background requirements of 10 CFR 73.56.

Protected Area Identification: 10 CFR 73.55(g)(6)

Guidelines

The physical security plan shall describe the numbered picture badge identification system provided for all individuals who are authorized unescorted access to the protected area.

The physical security plan shall indicate whether the site allows protected area identification badges to be removed from the protected area and the measures in place to ensure that the security badge is not compromised (e.g., badge deactivated upon exit, confirmation of identity and authorization before entry).

The physical security plan shall confirm that identification badges are clearly displayed while individuals are inside the protected area or vital areas. Implementing procedures should instruct employees to wear badges on the upper front portion of the body to be clearly visible except when operational safety concerns require otherwise.

The physical security plan shall confirm that a record is maintained that includes the names and affiliation of all individuals to whom photo identification badges have been issued and the areas to which unescorted access is granted. The physical security plan shall also confirm that a process to account for access control devices at least annually is established.

Visitor Access: 10 CFR 73.55(g)(7)

Guidelines

The physical security plan shall confirm that individuals who have not been granted unescorted access are escorted if granted access to a protected area or vital areas.

The physical security plan shall confirm that implementing procedures address the identification, processing, escorting, and training requirements for escorting visitors.

The physical security plan shall confirm that a visitor control register is maintained that includes the name, date, time, purpose of visit, employment affiliation, and citizenship of the visitor, and the name of the individual being visited.

The physical security plan shall confirm that a process has been established to confirm the identity of individuals requesting escorted access (visitors), in accordance with the requirements of 10 CFR 73.55(g)(7)(i)(B). Implementing procedures may contain further details.

The physical security plan shall confirm that personnel requesting visitor access to the protected area are not currently denied access to another licensed facility.

The physical security plan shall confirm that all visitors wear a badge that clearly indicates that an escort is required and that all visitors are escorted at all times.

Escorts: 10 CFR 73.55(g)(8)

Guidelines

The physical security plan shall confirm that all escorts are trained to perform escort duties in accordance with 10 CFR 73.55 and site requirements. The security plan shall also confirm that personnel escorts are provided with a means of timely communication with security personnel to summon assistance when needed. Within the training provided to personnel escorts, licensees should identify the communication assets available for use by the escorts and the location of the assets. Personnel acting as escorts for visitors should be generally knowledgeable about the activities performed by the visitor.

The physical security plan shall confirm that individuals acting as vehicle escorts are trained and qualified in accordance with Appendix B VI to 10 CFR Part 73 and are provided a means of continuous communication with security personnel.

The physical security plan shall describe visitor-to-escort ratios for protected areas and vital areas. Typical visitor-to-escort ratios are 10:1 for the protected area and 5:1 for vital areas.

Licensees shall describe visitor and vehicle escort observation and control requirements in implementing procedures.

Search Programs: 10 CFR 73.55(h)

Guidelines

The physical security plan shall describe the process for searching personnel, vehicles, and materials at predetermined locations before granting access to designated facility areas identified by the licensee, as needed, to satisfy the physical protection program requirements of 10 CFR 73.55(b).

Owner-Controlled Area Searches: 10 CFR 73.55(h)(2)

Guidelines

A physical security plan shall describe (as applicable) the owner-controlled area search process implemented at the OCA barrier checkpoint(s).

The physical security plan shall confirm that site implementing procedures exist for access control points for owner-controlled area barriers.

The physical security plan shall confirm that two trained and equipped security personnel are used to conduct vehicle searches at the access control point to the owner-controlled area. The security plan shall confirm that the armed individual is positioned to observe the search process and provide an immediate response.

The physical security plan shall confirm that vehicle searches are completed with the use of equipment capable of detecting firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage, or by a visual and physical search, or both, to ensure that all items are clearly identified before access is granted.

The physical security plan shall confirm that vehicle access control points are equipped with video surveillance equipment that is monitored by an individual capable of initiating a response.

Protected Area Searches: 10 CFR 73.55(h)(3)

Guidelines

The physical security plan shall confirm that the licensee implements personnel, material, and vehicle search processes to prevent the introduction of firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage into the protected area.

The physical security plan shall confirm that the search for firearms, explosives, incendiary devices, or other items that could be used to commit radiological sabotage is completed through the use of equipment capable of detecting these items or through visual and physical searches or both to ensure that all items are clearly identified before access is granted.

The physical security plan shall confirm that, with the exception of law enforcement personnel on official duty, all persons are subject to protected area entry searches. Armed security

officers who are on duty and have exited the protected area may reenter the protected area without being searched for firearms.

The physical security plan shall confirm that, when search equipment is out of service, not operating satisfactorily, or cannot be used effectively to search individuals that a visual and physical search is conducted.

The physical security plan should describe the actions taken when an attempt to introduce contraband into the protected area is suspected.

The physical security plan shall confirm that implementing procedures for vehicle access portals describe the areas of a vehicle that are searched before access is granted to the protected area.

The physical security plan shall describe the types of exceptions to be granted for materials and confirm that the specific security measures to be implemented for the excepted items are detailed in facility procedures.

The physical security plan shall confirm that bulk material excepted from protected area search is escorted by an armed member of the security organization to its final destination or to a receiving area where the excepted items are offloaded and verified and to the extent practicable are not offloaded adjacent to a vital area.

Detection and Assessment Systems: 10 CFR 73.55(i)

Guidelines

The physical security plan shall describe how detection and assessment systems satisfy 10 CFR 73.55(b) design requirements at all times to detect and assess unauthorized persons and support the effective implementation of the site protective strategy.

An acceptable physical security program would typically ensure that each detection system used to detect protected area intrusion is capable of detecting intrusions as identified in the system manufacturers testing specifications and the licensee testing and maintenance procedures.

The physical security plan shall confirm that alarm devices and transmission lines are tamper-indicating and self-checking and provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on backup power.

The physical security plan describes how the intrusion detection system is used to initiate a timely response in accordance with security plans, licensee protective strategy, and associated implementing procedures, to include the written protective strategy.

The physical security plan shall describe how the uninterruptible power supply maintains the intrusion detection and assessment equipment at the protected area perimeter as operable during the loss of normal power.

Alarm Stations: 10 CFR 73.55(i)(4)

Guidelines

The physical security plan shall confirm that two onsite alarm stations have detection equipment that annunciates and video assessment equipment that displays concurrently in both alarm stations.

The physical security plan shall confirm that a single act does not remove the capabilities of one alarm station to perform the functions of detection and assessment of alarms, initiate and coordinate an adequate response to an alarm, summon offsite assistance, and provide command and control.

The physical security plan shall confirm that at least one alarm station survives a single act to perform the required functions needed to successfully accomplish the goals and objectives of the site-specific protective strategy.

The physical security plan shall confirm that the alarm stations meet the descriptions listed in 10 CFR 73.55(i)(4)(i)(A) through (D).

The physical security plan shall confirm that the alarm stations meet the descriptions listed in 10 CFR 73.55(i)(4)(ii)(A) through (H).

Applicants for an operating license under the provisions of 10 CFR Part 50, or holders of a COL under the provisions of 10 CFR Part 52, shall confirm that both the central and secondary alarm stations are constructed, located, protected, and equipped to the standards for the central alarm station contained in 10 CFR 73.55. The physical security plan shall also confirm that both alarm stations shall be equal and redundant, such that all functions needed to satisfy the requirements of 10 CFR 73.55 for alarm stations can be performed in both alarm stations.

Surveillance, Observation, and Monitoring: 10 CFR 73.55(i)(5)

Guidance

The physical security plan shall describe the methods for surveillance, observation, and monitoring needed to satisfy the design requirements of 10 CFR 73.55(b), identify indications of tampering, or otherwise implement the site protective strategy.

The physical security plan shall describe the methods to continuously surveil, observe, and monitor the owner-controlled area to detect and deter intruders and to ensure the integrity of physical barriers or other components and functions of the onsite physical protection program.

The physical security plan shall confirm that unattended openings that intersect a security boundary, such as underground pathways, are protected by a physical barrier and monitored by intrusion detection equipment or observed by security personnel at a frequency to detect exploitation.

The physical security plan shall confirm that all exterior areas within the protected area are periodically checked by armed security patrols to detect the presence of unauthorized personnel

and material, as well as to inspect physical barriers and vital areas and their physical barrier portals. The physical security plan shall identify the frequency for this patrol.

The physical security plan shall confirm that all areas containing target sets are patrolled on a random basis. The security plan shall define the frequency of the patrol and the duties and responsibilities of the individual performing the patrol.

The physical security plan shall confirm that security personnel are trained to recognize obvious signs of tampering consistent with their duties and responsibilities. The physical security plan should describe other training provided to site personnel to assist with identifying and preventing tampering.

Illumination: 10 CFR 73.55(i)(6)

Guidelines

The physical security plan shall describe how the facility provides the illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and the implementation of the protective strategy.

The physical security plan shall describe how the licensee maintains the minimum illumination level of 0.2 foot-candles horizontally at ground level in isolation zones and defined exterior areas within the protected area.

If low-light technology is used to augment lighting to meet lighting requirements, the physical security plan shall describe the type of technology used and how it is incorporated into the site protective strategy and described in facility procedures.

Communications: 10 CFR 73.55(j)

Guidelines

The physical security plan shall describe how a continuous communications capability is maintained to ensure effective command and control with onsite and offsite resources during both normal and emergency situations.

The physical security plan shall describe how all on-duty security force personnel are capable of maintaining continuous communication with an individual in each alarm station and how vehicle escorts maintain continuous communication with security personnel.

The physical security plan shall confirm that personnel escorts maintain timely communications with security personnel and facility procedures should provide additional details for the communication methods provided to these types of escorts.

The physical security plan shall describe how, in addition to the conventional telephone service, the licensee provides continuous communication by establishing radio- or

microwave-transmitted two-way voice communication, either directly or through an intermediary, between local law enforcement and the site in both alarm stations, as required by 10 CFR 73.55.

The physical security plan shall confirm that both alarm stations required by 10 CFR 73.55 maintain a means of communication with the control room.

An acceptable physical security plan shall describe the independent power source provided for non-portable communications in the event of the loss of normal power.

The security plan shall confirm that areas of the site have been identified where communications could be interrupted or cannot be maintained, and that alternative communication measures have been established and addressed in facility procedures.

Response Requirements: 10 CFR 73.55(k)

Guidelines

The physical security plan shall confirm that properly trained, qualified, and equipped personnel are available at all times to interdict and neutralize threats, up to and including the DBT of radiological sabotage, as defined in 10 CFR 73.1.

The physical security plan shall confirm that firearms, ammunition, and equipment necessary to implement the site security plans and protective strategy are in sufficient supply and working order and are readily available to security personnel. The physical security plan should describe the firearms, ammunition, and equipment necessary to implement the site security plans and protective strategy.

The physical security plan shall confirm that each armed member of the security organization is trained to prevent or impede attempted acts of radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or under any other circumstances, as authorized by applicable State or Federal law.

The physical security plan shall describe duties and responsibilities of the security personnel used as armed responders and armed security officers to implement the site protective strategy within predetermined timelines.

For sites that use a remotely operated weapons system (ROWS), the physical security plan should also describe the duties and responsibilities of the ROWS operators, including operator actions and capabilities in the event the ROWS becomes inoperable during a contingency event.

The number of armed responders designated to implement the protective strategy shall not be less than 10, and the number of armed responders for the site shall be documented in the physical security plan.

The physical security plan shall confirm that the number of armed responders is sufficient to effectively implement the protective strategy, that they are available at all times inside the protected area (which may include the protected area access control point), and that they are not assigned other duties or responsibilities that could interfere with their assigned response duties.

The physical security plan shall confirm that armed security officers designated to strengthen the onsite response are on site and available at all times to carry out their assigned duties. The number of armed security officers designated to implement the protective strategy for the site shall be documented in the physical security plan.

For sites that use ROWS, the physical security plan should describe the number of ROWS employed at the site and the number of ROWS operators required to operate these systems (e.g. system to operator ratio), consistent with the implementation of the site protective strategy. The licensee should also describe the integration of the ROWS within the site's protective strategy, specifically stating whether these systems and the system operators are designated as a component of the minimum number of armed responders or of the armed security officers within the site's protective strategy.

The physical security plan should identify the number of armed security shift supervisors who may use the force continuum, including the use of deadly force, as authorized by applicable State law, for targets of opportunity and self-defense when implementing the site's protective strategy. If the licensee's physical security plan identifies armed security shift supervisors, these individuals must also be trained and qualified to perform armed duties in support of security-related and contingency events. For further information on armed security shift supervisors see NRC Staff White Paper "Duties and Responsibilities of the Security Shift Supervisor For Power Reactor Licensees," August 2009, ML100760663.

The physical security plan shall confirm that facility procedures provide a process to reconstitute the documented number of available armed response personnel required to implement the protective strategy. The physical security plan should document a specified timeframe to re-establish the minimum number of available armed response personnel.

Protective Strategy: 10 CFR 73.55(k)(8)

Guidelines

The physical security plan shall confirm that a written protective strategy is established that provides the methodology of the site's protective strategy to account for and protect the personnel, systems, and equipment needed to prevent significant core damage and spent fuel sabotage.

The physical security plan shall confirm that, upon receipt of an alarm or other indication of a threat, the licensee has pre-established methodologies and procedures to determine the existence and level of the threat and that facility procedures provide the details of this process.

The physical security plan shall confirm that response actions are initiated to interdict and neutralize threats in accordance with the requirements of 10 CFR Part 73, Appendix C, Section II, the safeguards contingency plan, and the site protective strategy.

The physical security plan shall confirm that local law enforcement is notified in accordance with facility procedures.

The protective strategy shall meet the requirements of 10 CFR Part 73, Appendix C, Section II.

Law Enforcement Liaison: 10 CFR 73.55(k)(9)

Guidelines

The physical security plan shall describe the process of documenting and maintaining the current law enforcement (local, State, and Federal) agreements, including estimated response times and the capabilities of the applicable law enforcement agencies. To the extent practicable, documentation of the law enforcement agreements should also include the number of personnel for response, available weapons, marshalling locations, command and control protocols, and frequency of training for law enforcement personnel contained in the site law enforcement response plan.

Heightened Security: 10 CFR 73.55(k)(10)

Guidelines

The physical security plan shall confirm that a threat warning system is established, maintained, and implemented which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. The security plan shall confirm that these measures and actions are consistent with the security plans and other emergency plans and procedures. The security plan shall confirm that upon notification by an authorized representative of the Commission, licensees shall implement the specific threat level indicated by the Commission representative.

Security Program Reviews: 10 CFR 73.55(m)

Guidelines

The physical security plan shall confirm that a review of the security program is conducted for each element of the program at least every 24 months.

The physical security plan shall confirm that a security program review is conducted within 12 months following initial implementation or when a change in personnel, procedures, equipment, or facilities could adversely affect security.

The physical security plan shall confirm that the security program review is completed by personnel who are independent of those responsible for program management and of any individual who has direct responsibility for implementing the onsite physical protection program.

The physical security plan shall confirm that the review of the security program, at a minimum, includes an audit of the effectiveness of the physical security program; security plans; implementing procedures; cyber security program; safety and security interface activities; testing, maintenance, and calibration program; and response commitments by local, State, and Federal law enforcement agencies.

The physical security plan shall confirm that the results and recommendations of the onsite physical protection program reviews, management findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews are documented in a report to the licensee plant manager and to corporate management at least one level higher than that having responsibility for day-to-day plant operations. The security plan shall confirm that these reports are maintained in an auditable form, available for inspection.

The physical security plan must confirm that findings from onsite physical protection program reviews must be entered into the site corrective action program.

Maintenance, Testing, and Calibration: 10 CFR 73.55(n)

Guidelines

The physical security plan shall confirm that the licensee has established a maintenance, testing, and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, are maintained in an operable condition, and are capable of performing their intended function.

The physical security plan shall confirm that implementing procedures specify the operation and technical details required to perform maintenance, testing, and calibration activities. Site maintenance, testing, and calibration procedures identify the criteria for determining when problems, failures, deficiencies, and other findings are documented in the site corrective action program for resolution.

The physical security plan shall confirm that effective compensatory measures are implemented when there is a failure or degraded operation of security-related components or equipment.

The physical security plan shall describe, at a minimum, that intrusion detection and assessment equipment, access control equipment, communications equipment, search equipment, security personnel equipment, firearms, and active vehicle barrier systems are tested and maintained as part of the site maintenance, testing, and calibration program.

The physical security plan shall confirm that each intrusion alarm is tested for operability at the beginning and end of any period that it is used for security. If the period of continuous use is longer than 7 days, the intrusion alarm should be tested at least once every 7 days.

The physical security plan shall confirm that onsite communications equipment is maintained in operational condition and tested for operability at least once at the beginning of each security personnel workshift.

The physical security plan shall confirm that equipment required for communications between alarm stations, each control room, and local law enforcement agencies, and backup communications equipment are tested at least once each day.

The physical security plan shall describe how search equipment is maintained in operational condition and is tested for operability at least once each day and tested for performance at least once during a 7 day period.

The physical security plan shall confirm that security personnel equipment is maintained in an operable condition with equipment checks or inspections to ensure that the equipment can perform the intended function.

The physical security plan shall confirm that a firearms maintenance program is established that includes the maintenance, testing, and accountability of all assigned licensee firearms. The physical security plan shall also confirm that the firearms maintenance program includes semiannual test firing for accuracy and functionality; firearms maintenance procedures that include cleaning schedules and cleaning requirements; program activity documentation; control and accountability (weapons and ammunition); firearms storage requirements; and armorer certification.

For sites that use an ROWS, the physical security plan shall confirm that the system components and associated firearms are included in the firearms maintenance program and that, at a minimum, the system is maintained, tested, calibrated, and the weapon test fired in accordance with the requirements of 10 CFR Part 73, Appendix B, Section VI, G.3., licensee procedures, and manufacturer's specifications.

The physical security plan shall confirm that the active vehicle barrier systems employed by the licensee, to include associated backup power supplies, are maintained in an operable condition and are tested in accordance with licensee procedures.

The physical security plan shall confirm that facility implementing procedures describe a program for testing or verifying the operability of devices or equipment located in hazardous areas, or that alternative measures are taken to ensure timely completion, or that testing or maintenance is conducted when hazardous conditions or other restrictions are no longer applicable.

The physical security plan shall confirm that security equipment or systems are tested in accordance with site maintenance, testing, and calibration procedures before being placed back in service after each repair or inoperable state.

Compensatory Measures: 10 CFR 73.55(o)

Guidelines

The physical security plan shall identify the criteria for instituting compensatory measures when security equipment, systems, or components become degraded or inoperable and the specific measures that provide an equivalent level of protection for the degraded or inoperable equipment, systems, and components.

The physical security plan shall identify the specific timeframe for implementing compensatory measures to ensure that degraded conditions do not decrease the effectiveness of the physical security program and protective strategy and continue to meet the general performance objective of 10 CFR 73.55(b).

Suspension of Safeguards Measures: 10 CFR 73.55(p)

Guidelines

The physical security plan must describe the process for the suspension of security measures. The process described in the security plan shall include the criteria within the provisions of 10 CFR 73.55(p) and 10 CFR 50.54(x) and (y).

Records: 10 CFR 73.55(q)

Guidelines

The physical security plan shall confirm that records on the following documents are maintained consistent with 10 CFR 73.55(q) and 10 CFR 73.70: access authorization records, suitability records, physical and mental qualification records for security personnel, protected area visitor access records; protected area vehicle access records; vital area access transactions; vitalization and devitalization records; vital area access list reviews; security plans and procedures; records of security patrols; inspections, tests, and maintenance records; alarm annunciation and security responses; records of liaison with local law enforcement agencies; records of audits and reviews; records of security-related access control devices; security training and qualification records; weapons testing, maintenance, and accountability records; the engineering analysis for the vehicle barrier system; and work hour control records.

The security plan shall describe the retention timeframe for records to be maintained in accordance with 10 CFR 73.55(q).

If a contracted security force is used at the site, the written contract agreements must be retained as a record for the duration of the contract.

The engineering analysis for the site vehicle barrier system(s) should be retained for the duration of the operating license.

Alternative Measures: 10 CFR 73.55(r)

Guidelines

The provision for alternative measures in 10 CFR 73.55(r) requires that, before implementation, these measures be submitted for NRC review and approval, in accordance with 10 CFR 50.4, "Written Communications," and 10 CFR 50.90, "Application for Amendment of License, Construction Permit, or Early Site Permit."

Licensee physical security plans should indicate when a specific measure described in the plan is an alternative measure and that the measure has been reviewed and approved by the NRC in accordance with 10 CFR 73.55(r), and 10 CFR 50.90.

Training and Qualification Plan

General Requirements and Introduction: 10 CFR Part 73, Appendix B VI, A.

Licensees shall require all individuals who are assigned duties and responsibilities required to prevent significant core damage and spent fuel sabotage to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures and to meet minimum training and qualification requirements to ensure that each individual possesses the knowledge, skills, and abilities (KSAs) required to effectively perform the assigned duties and responsibilities.

To ensure that those individuals who are assigned to perform duties and responsibilities required to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures are properly suited, trained, equipped, and qualified to perform their assigned duties and responsibilities, the Commission has developed minimum training and qualification requirements that must be implemented through a Commission-approved training and qualification plan.

The licensee shall establish, maintain, and follow a Commission-approved training and qualification plan. The training and qualification plan describes how the minimum training and qualification requirements set forth in Appendix B VI to 10 CFR Part 73 are met, to include the processes by which all individuals will be selected, trained, equipped, tested, and qualified.

Each individual assigned to perform security program duties and responsibilities required to effectively implement the Commission-approved security plans, licensee protective strategy, and licensee implementing procedures shall demonstrate the knowledge, skills, and abilities required to effectively perform the assigned duties and responsibilities before the individual is assigned the duty or responsibility.

Licensees 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.

A licensee may not allow any individual to perform security functions, assume security duties or responsibilities, or return to security duty until that individual satisfies the training and

qualification requirements of Appendix B VI to 10 CFR Part 73 and the Commission-approved training and qualification plan, unless specifically authorized by the Commission.

Annual training must nominally be scheduled within a 12 month period, but it may be completed up to 3 months before or 3 months after the scheduled date. However, the next annual training must be scheduled 12 months from the previously scheduled date, rather than the date the training was actually completed.

Employment Suitability and Qualification: 10 CFR Part 73, Appendix B VI, B.1.

Suitability

Guidelines

Consistent with 10 CFR Part 73, Appendix B, Section VI, B.1., individuals who are assigned security duties and responsibilities must meet minimum requirements to determine their initial and continued suitability (i.e., acceptability) and to ensure that they are and continue to be qualified (i.e., proven capable) to provide the required services before employment or assignment to the security organization.

The training and qualification plan shall confirm that all individuals employed for security duties, armed and unarmed positions, meet the requirements for suitability under 10 CFR Part 73, Appendix B, Section VI, B.1.

Physical Qualifications: 10 CFR Part 73, Appendix B VI, B.2.

Guidelines

The training and qualification plan shall confirm that personnel assigned security duties and responsibilities may not have any physical conditions that would adversely affect their performance of assigned duties and responsibilities and must demonstrate, before employment or assignment to the security organization, the necessary physical qualifications to effectively perform those assigned duties.

Medical Examinations and Physical Fitness Qualifications: 10 CFR Part 73, Appendix B VI, B.2.

Guidelines

The training and qualification plan shall confirm that armed and unarmed 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.

The training and qualification plan shall confirm that physical examinations are 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.

The training and qualification plan shall confirm that both armed and unarmed individuals who are assigned security duties and responsibilities identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures, meet the minimum physical requirements of 10 CFR Part 73, Appendix B, Section VI, B.2.(b) for vision, (c) for hearing, (d) for existing medical conditions, (e) for addiction, and (f) for those returning to duty from incapacitation caused by illness, injury, disease, or an operation.

Psychological Qualifications: 10 CFR Part 73, Appendix B VI, B.3.

Guidelines

The training and qualification plan shall confirm that security personnel meet the psychological qualifications in 10 CFR Part 73, Appendix B, Section VI, B.3., and that a licensed psychologist, psychiatrist, or physician trained, in part, to identify emotional instability shall determine whether armed members of the security organization and alarm station operators have an emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

Physical Fitness Tests: 10 CFR Part 73, Appendix B VI, B.4.

Guidelines

The training and qualification plan shall confirm that armed members of the security organization are subject to a medical examination by a licensed physician to determine if the individual is fit to participate in physical fitness tests.

The training and qualification plan shall confirm that, before assignment, armed members of the security organization shall demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test.

The training and qualification plan shall confirm that the licensee's physical fitness test considers physical conditions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security duties, for both normal and emergency operations, and that the test simulates site-specific conditions under which the individual will be required to perform assigned duties and responsibilities.

The training and qualification plan must describe the physical fitness test administered at the site in a manner that demonstrates that the test includes strenuous activity, physical exertion, levels of stress, and exposure to the elements and that it simulates site-specific conditions. Regulatory Guide 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," in the section entitled "Medical Examinations and Physical Fitness Test," contains additional details.

Physical Requalification: 10 CFR Part 73, Appendix B VI, B.5.

Guidelines

The training and qualification plan shall confirm that armed and unarmed individuals shall be required to demonstrate the capability to meet the physical requirements of 10 CFR Part 73, Appendix B, Section VI, and the licensee training and qualification plan at least annually and that this requalification is documented by a qualified training instructor and attested to by a security supervisor.

Duty Training: 10 CFR Part 73, Appendix B VI, C.1.

Guidelines

The training and qualification plan shall confirm that all personnel who are assigned to perform any security-related duty or responsibility are trained and qualified to perform assigned duties and responsibilities to ensure that each individual possesses the minimum KSAs required to effectively carry out those assigned duties and responsibilities.

The training and qualification plan shall confirm that individuals performing security duties are trained to perform assigned duties and responsibilities and meet the minimum qualification requirements of 10 CFR Part 73, Appendix B, Section VI, and the licensee training and qualification plan.

The training and qualification plan shall confirm that individuals performing security duties are trained and qualified in the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.

The training and qualification plan shall contain a list of critical job tasks (knowledge, skills, and abilities) for which individuals assigned to perform security duties must be trained and qualified. This listing should identify the specific duty positions within the security organization and the specific jobs for which individuals in each duty position are to be trained and qualified. The critical job task list (critical task matrix) provides a verification of the training and qualification that the individual in each duty position within the security organization is required to complete, along with the frequency of requalification and the specific method to be used for the qualification or requalification. The critical task matrix should be consistent with the training and qualifications required for the performance of specific security duties (e.g., armed security officers who are designated as a component of the protective strategy should be trained and qualified to respond to contingency events). RG 5.75 provides additional details concerning the list of job tasks for the training and qualification plan in the section entitled “Individual Training and Qualification for Duty.”

On-the-Job Training: 10 CFR Part 73, Appendix B VI, C.2.

Guidelines

The training and qualification plan shall confirm that individuals assigned duties to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures are provided on-the-job training (OJT) before performing their assigned duties.

The training and qualification plan shall confirm that individuals assigned duties and responsibilities to implement the safeguards contingency plan complete a minimum of 40 hours of OJT to demonstrate the knowledge, skills and abilities required to effectively perform assigned contingency duties and responsibilities in accordance with the safeguards contingency plans, protective strategy and implementing procedures. The training and qualification plan shall also confirm that OJT is documented by a qualified training instructor and attested to by a security supervisor.

The training and qualification plan shall confirm that OJT for contingency activities and drills must include, but is not limited to, hands-on application of knowledge, skills, and abilities related to:

- response team duties
- use of force
- tactical movement
- cover and concealment
- defensive positions
- fields-of-fire
- re-deployment
- communications (primary and alternative)
- use of assigned equipment
- target sets
- table top drills
- command and control duties, and
- licensee protective strategy

Performance Evaluation Program: 10 CFR Part 73, Appendix B VI, C.3.

Guidelines

The training and qualification plan shall confirm that the licensee has developed, implements, and maintains a performance evaluation program that is documented in procedures which describes how the licensee will demonstrate and assess the effectiveness of its onsite physical protection program and protective strategy, including the capability of the armed response team to carry out its assigned duties and responsibilities during safeguards contingency events.

The training and qualification plan should indicate that the performance evaluation program includes 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 and protective strategy. The training and qualification plan shall confirm that tactical response drills and force-on-force exercises are designed to challenge the site protective strategy against elements of the DBT and ensure that each participant assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures demonstrates the requisite KSAs.

The training and qualification plan shall confirm that tactical response drills, force-on-force exercises, and associated contingency response training are conducted under conditions that simulate, as closely as practicable, the site-specific conditions under which each member will, or may, be required to perform assigned duties and responsibilities.

The training and qualification plan shall confirm that tactical response drills and force-on-force exercises include a documented post-exercise critique in which participants identify failures, deficiencies, or other findings related to performance, plans, equipment, or strategies.

The training and qualification plan shall confirm that the licensee documents scenarios and participants for all tactical response drills and annual force-on-force exercises.

The training and qualification plan shall confirm that findings, deficiencies, and failures identified during tactical response drills and force-on-force exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program are entered into the licensee's corrective action program to ensure that timely corrections are made to the appropriate program areas.

The training and qualification program shall confirm that, during the conduct of tactical response drills and force-on-force exercises, only the total number of armed responders and designated armed security officers documented in the security plan are used; that artificialities are minimized; that systems or methodologies for the simulation of armed engagement are used; and that each scenario used provides a credible realistic challenge to the protective strategy and response organization.

The training and qualification plan shall confirm that the performance evaluation program is designed to ensure the following: each member of each shift who is assigned duties and responsibilities required to implement the safeguards contingency plan and licensee protective strategy participates in at least one tactical response drill on a quarterly basis and one force-on-force exercise on an annual basis; the mock adversary force replicates the adversary characteristics and capabilities of the DBT as closely as possible and is capable of challenging the licensees protective strategy; protective strategies can be evaluated by conducting tabletop drills and; drill and exercise controllers are trained and qualified to possess the requisite knowledge to control drills and exercises.

The training and qualification plan shall confirm that the licensee has developed and documented multiple scenarios for tactical response drills and force-on-force exercises; that the scenarios are designed to test and challenge any components or a combination of components of the physical protection program and protective strategy; and that each scenario uses a unique target set or target sets and adversary characteristics, so that all components of the

physical protection program and protective strategy are challenged, including but not limited to, equipment, implementing procedures, and personnel.

Duty Qualification and Requalification: 10 CFR Part 73, Appendix B VI, D.

Guidelines

The training and qualification plan shall confirm that armed and unarmed individuals shall demonstrate the required KSAs to carry out assigned duties and responsibilities, as stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures, and that this demonstration includes written exams and hands-on performance demonstrations.

The training and qualification plan should describe how written exams are administered, what the evaluation criteria are for written exams (e.g., minimum score of 80 percent to demonstrate acceptable understanding of assigned duties and responsibilities), and how performance demonstrations are conducted and evaluated.

The training and qualification plan shall confirm that an annual written exam is administered to armed members of the security organization and that the exam demonstrates that the members have the required KSAs to carry out their assigned duties and responsibilities.

The training and qualification plan shall include a description of the annual written exam, which in accordance with Regulatory Guide 5.75, “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities,” should, at a minimum, include the following elements and evaluation criteria :

- role of security personnel in supporting the safe operation of the facility
- use of deadly force, including the principles involved in the application, escalation, and de-escalation of force
- 10 CFR Part 73 requirements for the protection of SGI
- authority of private security personnel
- knowledge of who has the power of arrest and the authority to detain
- authority to search individuals and seize property
- offsite law enforcement response
- tactics and force that an adversary group might use to achieve its objectives
- response force deployment, tactical movement withdrawal, and use of support fire

The training and qualification plan shall confirm that personnel must achieve a minimum score of 80 percent on the annual written exam to demonstrate an acceptable understanding of assigned duties and responsibilities.

The training and qualification plan shall confirm that armed and unarmed individuals are requalified at least annually, in accordance with the requirements of 10 CFR Part 73, Appendix B, Section VI, and the Commission-approved training and qualification plan, and that the results of requalification are documented by a qualified training instructor and attested to by a security supervisor.

Weapons Training: 10 CFR Part 73, Appendix B VI, E.

General Firearms Training

Guidelines

The training and qualification plan must describe the weapons training program.

The training and qualification plan shall confirm that each armed member of the security organization is trained and qualified by a certified firearms instructor in the use and maintenance of each assigned weapon, including, but not limited to, marksmanship, assembly, disassembly, cleaning, storage, handling, clearing, loading, unloading, and reloading, for each assigned weapon. The training and qualification plan shall confirm that the licensee conducts annual firearms familiarization.

The training and qualification plan shall confirm that firearms' training is conducted by firearms instructors that are certified by a recognized national or State entity and that the certified firearms instructors are recertified in accordance with the standards recognized by the certifying national or State entity, but in no case shall recertification exceed 3 years.

The training and qualification plan shall confirm that the licensee's firearms training program includes the following:

- mechanical assembly, disassembly, weapons capabilities, and fundamentals of marksmanship
- weapons cleaning and storage
- combat firing, day and night
- safe weapons handling
- clearing, loading, unloading, and reloading
- firing under stress
- zeroing duty weapon(s) and weapons sighting adjustments

- target identification and engagement
- weapons malfunctions
- cover and concealment
- weapons familiarization

For sites that use ROWS, the training and qualification plan shall confirm that ROWS operators are provided training within the elements identified above, using the ROWS, as applicable.

The training and qualification program shall confirm that armed members of the security organization are instructed on the use of deadly force, as authorized by applicable State law.

The training and qualification plan shall confirm that each armed member of the security organization performs firearms training activities nominally every 4 months. Training may be conducted up to 5 weeks before and 5 weeks after the scheduled date. The next scheduled date must be 4 months from the originally scheduled date.

Weapons Qualification and Requalification Program: 10 CFR Part 73, Appendix B VI, F.

Guidelines

The training and qualification plan shall confirm that all armed members of the security organization are qualified and requalified on assigned weapons.

The training and qualification plan shall list the courses of fire and minimum score that must be achieved to demonstrate proficiency for each weapon used by armed personnel at the site. The training and qualification plan shall confirm that the results of weapons qualification and requalification are documented and retained as a record. At a minimum, the training and qualification plan shall confirm the following:

- Each course of fire used for the firearms qualification of armed members of the security organization with each assigned firearm (to include ROWS as applicable) is in accordance with standards established by a law enforcement course or an equivalent nationally recognized course.

- The annual daylight qualification courses of fire must consist of a qualifying score of 70 percent with a handgun and shotgun and 80 percent with a semiautomatic rifle and enhanced weapons. For sites that use ROWS, the system shall be included in the category of semiautomatic rifle or enhanced weapon (as applicable) for the required qualifying score.

- The annual night-fire qualification courses must consist of a qualifying score of 70 percent with a handgun and shotgun and 80 percent with a semiautomatic rifle and enhanced weapons. For sites that use ROWS, the system shall be included in the

category of semiautomatic rifle or enhanced weapon (as applicable) for the required qualifying score.

For tactical weapons qualification, the training and qualification plan must describe the firearms used, the firearms qualification program, and other tactical training required to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures. Licensee-developed tactical qualification and requalification courses must describe the performance criteria needed, to include site-specific conditions (e.g., lighting, elevation, fields of fire) under which assigned personnel shall be required to carry out their assigned duties.

The training and qualification plan shall confirm that the qualifying score for the annual tactical qualification course must be an accumulated total of 80 percent of the maximum obtainable score.

Consistent with Regulatory Guide 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," the training and qualification plan shall confirm that the licensee's tactical qualification course includes the following:

- the combined use of handguns and shoulder-fired weapons employed during a contingency event, according to the site's protective strategy
- firing from a reasonable and representative facsimile of licensee defensive positions, elevations, and distances
- appropriate levels of stress and physical demands (e.g., engaging targets while on the move)
- proper cover and concealment tactics while engaging multiple targets, moving targets, and decision making targets
- the ability to make the transition from one type of firearm to another
- the ability to recover from simulated weapon malfunctions (e.g., dummy rounds)
- adherence to the safe handling of firearms during simulated courses of fire
- firing at multiple targets and loading, and reloading while wearing a protective mask (gas mask)
- non-dominant (support) hand shooting
- use of the minimum quantity of ammunition for combined handgun and shoulder fired weapons necessary to demonstrate the ability to effectively implement the licensee's protective strategy

For sites that use ROWS, the training and qualification plan should identify the incorporation of ROWS within the tactical qualification course for ROWS operators as applicable.

Weapons, Personal Equipment, and Maintenance: 10 CFR Part 73, Appendix B VI, G.

Guidelines

The training and qualification plan shall confirm that armed personnel are provided with weapons that are capable of performing the function stated in the security plans, licensee protective strategy, and implementing procedures. The training and qualification plan should include a description of the firearm specifications and specific ammunition delivery mechanism (e.g. magazine fed, belt fed, drum fed, etc.) and number of rounds of the weapons employed at the site and that these firearms specifications are consistent with Appendix B to 10 CFR Part 73.

The licensee's training and qualification plan shall confirm that the firearms and ammunition employed at the site meet the minimum firearms and ammunition specifications (e.g., caliber, muzzle velocity, muzzle energy) of Appendix B to 10 CFR Part 73.

For sites that use ROWS, the training and qualification plan shall confirm that the specific firearm used in the ROWS meets the minimum firearms and ammunition specifications of Appendix B to 10 CFR Part 73 and includes a description of the firearm specifications and specific ammunition delivery mechanism (e.g. magazine fed, belt fed, drum fed, etc.) and number of rounds of the ROWS weapons employed at the site.

The training and qualification plan shall confirm that each individual is equipped with 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.

The training and qualification plan shall confirm that the licensee (at a minimum) provides armed security personnel, required for the effective implementation of the Commission-approved safeguards contingency plan and implementing procedures, with the following:

- gas mask, full face
- body armor (bullet-resistant vest)
- ammunition and equipment belt, and
- two-way portable radios, two channels minimum, one operating and one emergency

The training and qualification plan shall confirm that firearms (to include ROWS firearms, as applicable) are maintained in accordance with the requirements of 10 CFR Part 73, Appendix B, Section VI, G.3., and licensee implementing procedures and that personal equipment is maintained in accordance with licensee implementing procedures.

The training and qualification plan shall confirm that training and qualification records are retained in accordance with 10 CFR 73.55(q) and 10 CFR Part 73, Appendix B, Section VI, H., and licensee implementing procedures.

Safeguards Contingency Plan: 10 CFR Part 73, Appendix C, Section II

Nuclear Power Plant Safeguards Contingency Plans

The safeguards contingency plan is a documented plan that describes how licensee personnel implement their physical protection program to defend against threats to their facility, up to and including the DBT of radiological sabotage.

The goals of licensee safeguards contingency plans are the following:

- to organize the response effort at the licensee level
- to provide predetermined, structured responses by licensees to safeguards contingencies
- to ensure the integration of the licensee response by other entities, and
- to achieve a measurable performance in response capability. Licensee safeguards contingency planning should result in organizing the licensee's resources in such a way that the participants will be identified, their responsibilities specified, and the responses coordinated

The responses should be timely and include personnel who are trained and qualified to respond in accordance with a documented training and qualification program. The evaluation, validation, and testing of this portion of the program shall be conducted in accordance with Appendix B to 10 CFR Part 73.

The licensee's safeguards contingency plan is intended to maintain effectiveness during the implementation of emergency plans developed under Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities," to 10 CFR Part 50.

Guidelines

The safeguards contingency plan should generally describe relationships and interactions among the safeguards contingency plan, the physical security plan, and the training and qualification plan, and with other non-security plans as they relate to the overall physical protection program. Detailed technical information required to establish or support the technical basis for actions, described in the safeguards contingency plan but not required to understand or implement the plan, may also be captured through reference to applicable documentation, rather than by specific inclusion in the safeguards contingency plan.

The general description of the safeguards contingency plan should contain actions and objectives to be accomplished by the security organization and explain how the stated actions and objectives are coordinated with actions that may be performed concurrently by other onsite entities, such as operations and fire protection, to avoid potential conflicts during security-related contingency events or other emergency situations that could directly or indirectly endanger the public health and safety or common defense and security.

The safeguards contingency plan must contain a level of information regarding contingency situations, in general, sufficient to ensure an understanding of duties and responsibilities necessary to effectively deal with and counter identified contingency events.

The safeguards contingency plan is designed and implemented to provide protection against the DBT of radiological sabotage, as described in 10 CFR 73.1 and associated adversary characteristics. RG 5.69 contains additional guidance regarding adversary characteristics of the DBT of radiological sabotage.

The safeguards contingency plan, at a minimum, will describe the following areas: background, generic planning base, licensee planning base, responsibility matrix, and implementing procedure descriptions. The licensee need not submit implementing procedures to the NRC.

Background: 10 CFR Part 73, Appendix C II, B.1.

Guidelines

The background shall describe, at a minimum, the following areas in the safeguards contingency plan: purpose and scope of the plan, perceived danger (general description of the threat posed by the DBT), and any applicable definitions.

Generic Planning Base: 10 CFR Part 73, Appendix C II, B.2.

Guidelines

The safeguards contingency plan shall contain a generic planning base that identifies 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 licensee personnel. The generic planning base should address event initiation, such as the detection of unauthorized activities; the response to all alarms or other indications signaling a security event, such as penetration of a protected area, vital area, or unauthorized barrier penetration (vehicle or personnel); tampering; and bomb threats or other threat warnings—either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

The generic planning base within the safeguards contingency plan shall describe specific threats or events and list the objectives to be accomplished for each event identified. The generic planning base shall also identify the data, criteria, procedures, mechanisms, and logistical support required for the evaluation and response to each event described.

RG 5.54, “Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants,” outlines the generic situations that are captured in a licensee’s contingency plan. The licensee’s site implementing procedures must address the decisions and actions of response for each event.

Licensee Planning Base: 10 CFR Part 73, Appendix C II, B.3.

Guidelines

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.

The planning base must contain the following areas: organizational structure, physical layout, safeguards systems, law enforcement assistance, policy constraints and assumptions, and administrative and logistical considerations.

Organizational Structure: 10 CFR Part 73, Appendix C II, B.3.a.

Guidelines

The safeguards contingency plan must describe the chain of command and delegation of authority for the security organization during safeguards contingency events, to include a general description of the implementation of the command and control functions. The safeguards contingency plan should contain a general duty description for members of the security response organization during a contingency event.

Physical Layout: 10 CFR Part 73, Appendix C II, B.3.b.

Guidelines

The safeguards contingency plan or physical security plan must contain a map that depicts the physical structures located on the site, including onsite independent spent fuel storage installations if applicable, and a description of the structures depicted on the map. The map shall also depict nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may affect response activities. These maps should indicate the main and alternate routes for law enforcement or other offsite response and support agencies and locations for marshalling coordination responses.

Safeguards Systems: 10 CFR Part 73, Appendix C II, B.3.c.

Guidelines

The safeguards contingency plan must describe how a licensee will respond to an event to protect against the DBT, as described in 10 CFR 73.1(a). The description by the licensee must be consistent with 10 CFR Part 73, Appendix C II, (B)(3)(c)(v) and include the physical protection program measures implemented from the outermost facility perimeter inward to the measures that protect target set equipment. (The description should start from the owner-

controlled area to the protected area and end at vital areas.) This description must have the following elements:

- Defense in depth (e.g., physical barriers, alarm systems, locks, area access, armaments, surveillance, communication systems). COL applicants that use security design technical reports to establish their protective strategy should capture key security design features in the safeguards contingency plan description that are relied on to effectively implement the site protective strategy (e.g., supplemental fence locations and additional security features that are specific to the nuclear island design).

- Structure of the security response organization. The number of armed responders designated to implement the protective strategy (which shall not be less than 10) shall be documented in the safeguards contingency plan. The number of armed security officers designated to implement the protective strategy for the site shall be documented in the safeguards contingency plan. For sites that use ROWS, the safeguards contingency plan should describe the number of ROWS employed at the site and the number of ROWS operators that are required to operate these systems (e.g. system to operator ratio), consistent with the implementation of the site protective strategy. The licensee should also state whether these systems and the system operators are designated as a component of the minimum number of armed responders or designated armed security officers within the site's protective strategy.

- Armed response team duties and responsibilities. The safeguards contingency plan shall describe the duties and responsibilities of the security personnel used as armed responders and armed security officers to implement the site protective strategy within predetermined timelines. For sites that use ROWS, the duties and responsibilities of the ROWS operators should also be described in the safeguards contingency plan. This description should include operator actions and capabilities, in the event ROWS becomes inoperable during a contingency event.

- Written protective strategy. This written facility procedure describes the methodology to determine the existence and level of a threat, the deployment and function of the response organization (to include ROWS, if applicable) to implement the licensee protective strategy, and specific details of offsite law enforcement agency support and capabilities.

Law Enforcement Assistance: 10 CFR Part 73, Appendix C II, B.3.d.

Guidelines

The safeguards contingency plan shall include a list of available law enforcement agencies and a general description of their response capabilities and their criteria for response, as well as a discussion of working agreements or arrangements for communicating with these agencies.

Policy Constraints and Assumptions: 10 CFR Part 73, Appendix C II, B.3.e.

Guidelines

The safeguards contingency plan shall contain a discussion of State laws, local ordinances, and company policies and practices that govern the licensee response to incidents and must include, but is not limited to, the following:

- use of deadly force
- recall of off-duty employees
- site jurisdictional boundaries, and
- use of enhanced weapons, if applicable

Responsibility Matrix: 10 CFR Part 73, Appendix C II, B.4.

Guidelines

The licensee's safeguards contingency plan shall reference the responsibility matrix and include a description of responsibility matrix procedures. This description should include the detailed identification of responsibilities and specific actions to be taken by licensee organizations and personnel in response to safeguards contingency events. The safeguards contingency plan shall confirm that the predetermined actions identified in the responsibility matrix procedures can be completed under the postulated conditions.

Licensees shall develop site procedures that consist of matrixes detailing the organization and personnel responsible for decisions and actions associated with specific responses to safeguards contingency events. Responsibility matrix procedures shall be based on the events outlined in the generic planning base.

Implementing Procedures: 10 CFR Part 73, Appendix C II, B.5.

Guidelines

Licensees shall establish and maintain written implementing procedures that provide specific guidance and operating details to 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.

IV. EVALUATION FINDINGS

The reviewer should verify that the applicant has provided sufficient information and that the review and calculations (if applicable) support conclusions of the following type to be included in the staff's safety evaluation report. The reviewer should also state the basis for these conclusions.

The evaluation finding(s) should be substantially equivalent to the following statement:

> A security plan has been submitted for the protection of the plant against potential acts of radiological sabotage. The security plan has been withheld from public disclosure pursuant to 10 CFR 2.390(d).
>
> The applicant/licensee described the physical security program and the insider mitigation program based on 10 CFR 73.55; the training and qualification program and the performance evaluation program based on 10 CFR Part 73, Appendix B VI; the safeguards contingency plan based on 10 CFR Part 73, Appendix C II; the access authorization program based on 10 CFR 73.56; and the implementation of these programs and measures in conformance with the listed regulations.
>
> The security plan has been reviewed for format and content using the most recent NRC-endorsed revision of NEI 03-12 Security Plan Template, which contains all features considered essential for such a program by the staff, and is acceptable. In particular, it has been found to comply with the Commission's regulations, including 10 CFR Part 26; 10 CFR 50.34(c) and (d); 10 CFR 52.79(a)(35)(i), (a)(36)(i), and (a)(36)(ii); and applicable sections of 10 CFR Part 73, including Appendix B and Appendix C.

For COL reviews, the findings should also summarize the staff's evaluation of requirements and restrictions (e.g., interface requirements and site parameters) and COL action items relevant to this SRP section.

V. IMPLEMENTATION

The staff may use this SRP section in performing safety evaluations of DC applications and license applications submitted by applicants pursuant to 10 CFR Part 50 or 10 CFR Part 52. Except when the applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the staff will use the method described here to evaluate conformance with Commission regulations.

VI. REFERENCES

1. 10 CFR Part 26, "Fitness for Duty Programs."

2. 10 CFR 50.4, "Written Communications."

3. 10 CFR 50.34(c)(2), "Physical Security Plan, and Training and Qualification Plan."

4. 10 CFR 50.34(d)(2), "Safeguards Contingency Plan."

5. 10 CFR 50.54(p), "Conditions of Licenses."
6. 10 CFR 50.70(b)(3), "Inspections."

7. 10 CFR 50.90, “Application for Amendment of License, Construction Permit, or Early Site Permit.”

8. 10 CFR 52.79(a)(35), “Physical Security Plan.”

9. 10 CFR 52.79(a)(36), “Training and Qualification Plan.”

10. 10 CFR 52.79(a)(36), “Safeguards Contingency Plan.”

11. 10 CFR Part 73, “Physical Protection of Plants and Materials.”

12. 10 CFR 73.1, “Purpose and Scope.”

13. 10 CFR 73.2, “Definitions.”

14. 10 CFR 73.21, §73.22, §73.23, “Requirements for the Protection of Safeguards Information.”

15. 10 CFR 73.55, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.”

16. 10 CFR 73.56, “Personnel Access Authorization Requirements for Nuclear Power Plants.”

17. 10 CFR 73.57, “Requirements for Criminal History Record Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information.”

18. 10 CFR 73.70, “Records.”

19. 10 CFR 73.71, “Reporting of Safeguards Events.”

20. 10 CFR Part 73, Appendix B, “General Criteria for Security Personnel.”

21. 10 CFR Part 73, Appendix C, “Nuclear Power Plant Safeguards Contingency Plans.”

22. 10 CFR Part 73, Appendix G, “Reportable Safeguards Events.”

23. 10 CFR Part 73, Appendix H, “Weapons Qualification Criteria.”

24. RG 1.206, “Combined License Applications for Nuclear Power Plants.”

25. RG 5.54, “Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants.”

26. RG 5.66, “Access Authorization Program for Nuclear Power Plants.”

27. RG 5.69 “Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program That Meets 10 CFR 73.55 Requirements”

28. RG 5.75, “Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities.”

29. RG 5.76, “Physical Protection Programs at Nuclear Power Reactors.”

30. RG 5.77, “Insider Mitigation Program.”

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52, and were approved by the Office of Management and Budget, approval number 3150 0011 and 3150 0151.

PUBLIC PROTECTION NOTIFICATION

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

APPENDIX I
PHYSICAL SECURITY PLAN

NEI 03-12 TEMPLATE Physical Protection Plan (PSP) SECTION TITLE	SECURITY REGULATIONS
Introduction and Facility Layout	10 CFR 73.55(a) and (c), 10 CFR 73, Appendix C, Section II, B.3.(b)
Performance Objectives	10 CFR 73.55(a) through (k)
Performance Evaluation Program	10 CFR Part 73, Appendix B, Section VI, C.3.(a) through (l); 10 CFR 73.55(b)(6)
Establishment of Security Organization	10 CFR 11.11; 10 CFR 73.55(d); 10 CFR Part 73, Appendix C, Section II, B.3.(a)
Qualification for Employment in Security	
1. Training and Facility Personnel	10 CFR 73.55(c)(4); 10 CFR 73.55(d)(3); 10 CFR 50.120; 10 CFR Part 73, Appendix B, Section VI
2. Security Personnel training	10 CFR Part 73, Appendix B, Section VI
3. Local Law Enforcement Liaison	10 CFR 73.55(k)(9); 10 CFR Part 73, Appendix C, Section II
4. Security Personnel Equipment	10 CFR Part 73, Appendix B, Section VI, G.2
5. Work-Hour Controls	10 CFR Part 26, Subpart I
Physical Barriers	
1. Vehicle Barrier System (VBS)	10 CFR 73.55(e)(10)
2. Channeling Barrier System (as applicable-site specific)	10 CFR 73.55(e)(6)
3. Protected Area (PA) Barrier	10 CFR 73.55(e)(8)
4. Vital Area (VA) Barrier	10 CFR 73.55(e)(9)
5. Delay Barriers	10 CFR 73.55(e)(3)(C)(ii) and (iii)
Target Sets	10 CFR 73.55(f)
Security Posts and Structures	10 CFR Part 73, Appendix C, Section II,

	B.3.c(v)(3)
Access Requirements	
1. Access Authorization and Fitness for Duty	10 CFR 73.56, 10 CFR Part 26
2. Insider Mitigation Program	10 CFR 73.55(b)(9)
3. Picture Badge Systems	10 CFR 73.55(g)(6)(ii)
4. Searches	
a. VBS Access Control Point	10 CFR 73.55(h)(2)
b. Packages and Materials	10 CFR 73.55(h)(3)
c. PA Vehicle Search	10 CFR 73.55(h)(3)
d. PA Personnel Search	10 CFR 73.55(h)(3)
5. PA Access Controls	10 CFR 73.55(g); 10 CFR 73.56
a. Escort and Visitor Requirements	10 CFR 73.55(g)(7)
6. VA Access Controls	10 CFR 73.55(g)(4)
7. Waterborne Threat Measures	10 CFR 73.55(e)(10)(ii)
Surveillance, Observation, Monitoring	
1. Illumination	10 CFR 73.55(i)(6)
2. Surveillance	10 CFR 73.55(i)(5)
3. Intrusion Detection Equipment	10 CFR 73.55(i)(1)(2)(3)
4. CAS and SAS Operation	10 CFR 73.55(i)(4)
5. Security Patrols	10 CFR 73.55(i)(5)
a. OCA	Same as above
b. PA and VA	Same as above
Communications	

1. Notifications 2. System Descriptions	10 CFR 73.55(j); 10 CFR 73.55(k)(8)(iii) Same as above
Review, Evaluation, and Audit of the Security Program	10 CFR 73.55(m)
Response Requirements	10 CFR 73.55(k)
Special Situations Affecting Security 1. Refueling/Major Maintenance 2. Construction and Maintenance	 10 CFR 73.55(b)(3)(i) Same as above
Testing and Maintenance 1. Intrusion Detection & Access Control Devices 2. Search Equipment 3. Communications Equipment 4. Security Personnel Equipment 5. Firearms 6. Active Vehicle Barrier System	 10 CFR 73.55(n) Same as above Same as above Same as above Same as above; 10 CFR Part 73, Appendix B, Section VI, G.3 10 CFR 73.55(e)(10)(i)(B)
Compensatory Measures 1. PA Physical Barriers 2. VA Barriers 3. Perimeter Intrusion Detection Alarm System 4. PA Lighting 5. VA Portal Alarms 6. Closed Circuit Television/Nonfixed Camera System	 10 CFR 73.55(o); 10 CFR Part 73, Appendix G, reportable safeguard events, Sections I and II Same as above Same as above Same as above Same as above Same as above

7. Playback/Recorded Video System	Same as above
8. Security Computer System	Same as above
9. PA Device	Same as above
10. Vehicle Barrier System	Same as above
11. Channeling Barrier System (as applicable—site specific)	Same as above
12. Other Security Equipment	Same as above
Records	10 CFR 73.70, 10 CFR 73.55(q)
1. Access Authorization Records	10 CFR 73.55(g)(4)(i), 10 CFR 73.56(o)
2. Suitability, Physical, and Psychological Qualification Records for Security Personnel	10 CFR Part 73, Appendix B, Section VIB
3. PA and VA Access Control Records	10 CFR 73.70(a) and (b)
a. PA Visitor Access Records	10 CFR 73.70(c)
b. VA Access Transactions Records	10 CFR 73.70(d)
c. Vitalization and Devitalization Records	10 CFR 73.55(q)
d. Vital Area Access List Review	10 CFR 73.56(j)
4. Security Plans and Procedures	10 CFR 73.55(q)(2)
5. Security Patrols, Inspections, and Tests	10 CFR 73.70(e)
6. Maintenance	10 CFR 73.70(e)
7. CAS/SAS Alarm Annunciation and Security Responses	10 CFR 73.70(f); 10 CFR 73.55(q)(2)
8. LLEA Liaison	10 CFR 73.55(k); 10 CFR Part 73, Appendix C, Section II, B.3.d
9. Record of Audits and Reviews	10 CFR 73.55(q)(4)
10. Records of Security-Related Keys	10 CFR 73.70(e) and (h)

11. Security Training and Qualification Records	10 CFR Part 73, Appendix B; 10 CFR 73:70
12. Firearms Testing and Maintenance Records	10 CFR 73.70(e), 10 CFR Part 73, Appendix B, Section VI, G.3
13. Engineering Analysis for the Vehicle Barrier System	10 CFR 73.55(e)(2); 10 CFR 73.70; 10 CFR 73.55(c)(7) and (8); 10 CFR 73.21, 10 CFR 73 22
Digital Systems Security	10 CFR 73.54; 10 CFR 73.55(b)(8)
Temporary Suspension of Security Measures	
1. Suspension of Security Measures	10 CFR 73.55(p); 10 CFR 50.54; 10 CFR 73.71; 10 CFR 50.72
2. Suspension of Security Measures During Severe Weather or Other Hazardous Conditions	10 CFR 73.55(p)
3. Notification	10 CFR 73.55(p), 10 CFR 73.71, 10 CFR 50.72

APPENDIX II
TRAINING AND QUALIFICATION PLAN

NEI 03-12 TEMPLATE Physical Protection Plan (PSP) SECTION TITLE	SECURITY REGULATIONS
Introduction	10 CFR 73.55(b)(3)(i) and (6); 10 CFR 73.55(d)(1) and (3); 10 CFR Part 73, Appendix B
Employment Suitability and Qualification	10 CFR Part 73, Appendix B, Section VI, A and B
1. Suitability	Same as above
2. Physical Qualifications	Same as above
3. Physical Examination	Same as above
4. Armed Personnel Requirements	Same as above
a. Vision	Same as above
b. Hearing	Same as above
c. Diseases	Same as above
d. Addiction	Same as above
e. Other Physical Requirements	Same as above
5. Psychological Qualifications	10 CFR Part 73, Appendix B, Section VI, B.3
6. General Psychological Qualifications	Same as above
7. Professional Psychological Examination	Same as above
8. Documentation	10 CFR Part 73, Appendix B, Section VI, H.3
9. Physical Requalification	10 CFR Part 73, Appendix B, Section VI, B.5
Individual Training and Qualification	10 CFR Part 73, Appendix B
Duty Training	10 CFR Part 73, Appendix B, Section VI, C
On-the-Job Training	10 CFR Part 73, Appendix B, Section VI, C.2
Critical Task Matrix	10 CFR Part 73, Appendix B, Section VI, D.1

a. Watchperson	Same as above
b. Armed Security Officer	Same as above
c. Armed Responder	Same as above
d. Alarm Station Operator	Same as above
e. Response Team Leader	Same as above
f. Security Shift Supervisor	Same as above
Initial Training and Qualification Requirements	10 CFR 73.55(d)(1); 10 CFR Part 73, 10 CFR, Appendix B, Section VI
Written Examination	10 CFR Part 73, Appendix B, Section VI, D.1(b)(1)
Hands-on Performance Demonstration	10 CFR Part 73, Appendix B, Section VI, D.1(b)(2)
Continuing Training and Qualification	10 CFR 73.55(d)(1) and (3); 10 CFR Part 73, Appendix B, Section VI
1. Annual Written Exams	10 CFR Part 73, Appendix B, Section VI, D.1(b)(3)
2. Demonstration of Skills and Ability	10 CFR Part 73, Appendix B, Section VI, D.1(b)(2)
3. Physical Fitness	10 CFR Part 73, Appendix B, Section VI, B.4
4. Documentation	10 CFR Part 73, Appendix B, Section VI, B.4(b)(4)
Weapons Training and Qualification	10 CFR Part 73, Appendix B, Section VI, E
1. General Firearms Training	10 CFR Part 73, Appendix B, Section VI, E.1
2. General Weapons Qualifications	10 CFR Part 73, Appendix B, Section VI, F.1
3. Tactical Weapons Qualification	10 CFR Part 73, Appendix B, Section VI, F.2
4. Firearms Qualification Courses	10 CFR Part 73, Appendix B, Section VI, F.3
5. Courses of Fire	10 CFR Part 73, Appendix B, Section VI, F.4
6. Firearms Requalification	10 CFR Part 73, Appendix B, Section VI, F.5
7. Weapons, Personal Equipment, and Maintenance	10 CFR Part 73, Appendix B, Section VI, G
8. Documentation	10 CFR Part 73, Appendix B, Section VI, F.1(b)

Performance Evaluation Program	10 CFR Part 73, Appendix B, Section VI, C.3

APPENDIX III
SAFEGUARDS CONTINGENCY PLAN

NEI 03-12 TEMPLATE Physical Protection Plan (PSP) SECTION TITLE	SECURITY REGULATIONS
Background Information	10 CFR 50.34(d); 10 CFR Part 73, Appendix C II; 10 CFR 73.55(k)(1)
1. Purpose of SCP	10 CFR Part 73, Appendix C II, B.1.b
2. Scope of SCP	10 CFR Part 73, Appendix C II, B.1.c
3. Perceived Danger	10 CFR Part 73, Appendix C II, B.1.a
Generic Planning Base	10 CFR Part 73, Appendix C II, B.2
1. Situations Not Covered by SCP	Same as above
2. Situations Covered by SCP	Same as above
3. Responsibility Matrix	10 CFR Part 73, Appendix C II, B.4
Licensee Planning Base	10 CFR Part 73, Appendix C II
1. Licensee Organization	10 CFR Part 73, Appendix C II, B.3.a
2. Physical Layout	10 CFR Part 73, Appendix C II, B.3.b
3. Safeguards Systems	10 CFR Part 73, Appendix C II, B.3.c; 10 CFR 50.54(p)(1) and (2)
4. Law Enforcement Assistance	10 CFR Part 73, Appendix C II, B.3.d
5. Policy Constraints and Assumptions	10 CFR Part 73, Appendix C II, B.3.e
6. Administrative and Logistical Considerations	10 CFR Part 73, Appendix C II, B.3.f
Response Capabilities	
1. Response to Threats	10 CFR 73.55(k)
2. Armed Response Team	10 CFR Part 73, Appendix B VI; 10 CFR Part 73, Appendix C II, B.3.; 10 CFR 73.55(k)(4) and (5)
3. Supplemental Security Officer	Same as above

4. Facility Operations Response 5. Emergency Plan Response 6. Local Law Enforcement Agencies (LLEAs) 7. State Response Agencies 8. Federal Response Agencies 9. ISFSI	10 CFR Part 73, Appendix C II 10 CFR Part 73, Appendix C II 10 CFR Part 73, Appendix C II, B.3.d; 10 CFR 73.55(k) Same as above Same as above
Defense in Depth	10 CFR 73.55, 10 CFR Part 73, Appendix C II, B.3.c
Primary Security Functions	10 CFR 73.55(a) through (k); 10 CFR Part 73, Appendix C, Section II, B.3
Protective Strategy Scenarios	10 CFR Part 73, Appendix C II; 10 CFR Part 73 Appendix B VI, C.3

SRP Section 13.6.1
"Physical Security – Combined License and Operating Reactors"
Description of Changes

This Revision 1 to SRP Section 13.6.1, dated June 2010, updates the initial issuance of this section, dated March 2007, to reflect the changes of the recently issued 10 CFR Part 73, Power Reactor Security Rule (published in the *Federal Register* (FR) on March 27, 2009 (74 FR 13926)).

The technical changes in accordance with the new 10 CFR Part 73 Rule are incorporated in each section of this revision (Revision 1, dated June 2010) of the SRP as applicable.