

NUREG-1615

Physical Protection Requirements for Categories I, II, and III Material at Fuel Cycle Facilities

**Manuscript Completed: February 1999
Date Published: March 1999**

C. Brown

**Division of Fuel Cycle Safety and Safeguards
Office of Nuclear Material Safety and Safeguards
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001**

ABSTRACT

This NUREG presents the primary physical protection requirements, issued by the U.S. Nuclear Regulatory Commission (NRC), under Title 10 of the U.S. Code of Federal Regulations, applicable to unirradiated Categories I, II, and III material at fixed sites. Category I refers to formula quantities of strategic special nuclear material. Category II refers to quantities and types of special nuclear material of moderate strategic significance. Category III refers to quantities and types of special nuclear material of low strategic significance. The requirements are presented in a modular format in relation to the various physical protection functional areas.

TABLE OF CONTENTS

| | |
|---|-----|
| ABSTRACT | iii |
| Table of Contents | v |
| 1. INTRODUCTION | 1 |
| 1.1 Purpose | 1 |
| 1.2 Scope of NUREG | 1 |
| 1.3 Additional Guidance | 1 |
| 1.4 Modular Format | 1 |
| 1.5 Description of NUREG | 1 |
| 2. PHYSICAL PROTECTION PLAN COMPONENT MODULE | 3 |
| 2.1 Module I : General Requirements | 3 |
| 2.1.1 Physical Protection Plans | 3 |
| 2.1.2 Implementation | 3 |
| 2.1.3 Records | 4 |
| 2.2 Module II: General Performance Objectives and Capabilities | 6 |
| 2.2.1 Performance Objectives | 6 |
| 2.2.2 Performance Capabilities | 6 |
| 2.3 Module III: Threat and Protection Goal | 9 |
| 2.3.1 Threat and Protection Goal | 9 |
| 2.4 Module IV: Security Organization | 11 |
| 2.4.1 Establishment of Security Organization | 11 |
| 2.4.2 Response Force | 12 |
| 2.4.3 Security Organization Management | 13 |
| 2.4.4 Qualifications for Employment in Security | 14 |
| 2.4.5 Guard Force Training | 15 |
| 2.4.6 Physical Fitness Testing | 17 |
| 2.4.7 Fitness-For-Duty Programs | 24 |
| 2.4.8 Medical Requirements | 24 |
| 2.4.9 Security Force Armament | 26 |
| 2.4.10 Force-on-Force Exercises | 26 |
| 2.4.11 Records | 28 |
| 2.5 Module V: Barriers and Designated Areas | 29 |
| 2.5.1 PA and Controlled Access Area Barriers | 29 |
| 2.5.2 Vehicle Barriers | 29 |
| 2.5.3 MAA and Controlled Access Area Barriers | 30 |
| 2.5.4 Isolation Zones | 30 |
| 2.5.5 Illumination | 31 |
| 2.5.6 Storage of Nuclear Material | 31 |
| 2.5.7 Storage of Enriched Uranium Scrap | 33 |
| 2.6 Module VI: Access Control Subsystems and Procedures | 34 |
| 2.6.1 Numbered Picture Badge System | 34 |
| 2.6.2 Access to MAA and Controlled Access Areas | 35 |

| | | |
|-------------|--|-----------|
| 2.6.3 | Access Controls at the PA for: | 35 |
| 2.6.3.1 | Personnel | 35 |
| 2.6.3.2 | Hand-Carried Packages | 37 |
| 2.6.3.3 | Delivered Packages | 37 |
| 2.6.3.4 | Vehicles | 38 |
| 2.6.4 | Access Controls at MAAs and Controlled Access Areas for: | 39 |
| 2.6.4.1 | Personnel | 39 |
| 2.6.4.2 | Packages | 40 |
| 2.6.4.3 | Vehicles | 40 |
| 2.6.5 | MAA Exit Search of Contaminated Waste | 41 |
| 2.6.6 | Preparing SSNM for Shipment Offsite | 41 |
| 2.6.7 | Escorts and Escorted Individuals | 42 |
| 2.6.8 | Keys, Locks, and Combinations | 42 |
| 2.6.9 | Records | 43 |
| 2.7 | Module VII: Detection, Surveillance, and Alarm Subsystems | 45 |
| 2.7.1 | Isolation Zone Penetration | 45 |
| 2.7.2 | Emergency Exits | 45 |
| 2.7.3 | MAA and Controlled Access Area Protection | 46 |
| 2.7.4 | Duress Alarms | 47 |
| 2.7.5 | Central and Secondary Alarm Stations | 47 |
| 2.7.6 | Power Sources | 49 |
| 2.7.7 | Component Supervision | 49 |
| 2.7.8 | External PA Monitoring and Assessment | 50 |
| 2.7.9 | Observation Methods within MAA and Controlled Access Areas | 50 |
| 2.7.10 | Records | 51 |
| 2.8 | Module VIII: Communications Subsystems | 52 |
| 2.8.1 | Security Force Communications | 52 |
| 2.8.2 | Alarm Station Communications | 52 |
| 2.8.3 | Independent Power Sources for Communications Equipment | 52 |
| 2.9 | Module IX: Test and Maintenance Program for | |
| | Physical Protection Equipment | 53 |
| 2.9.1 | Test and Maintenance Program | 53 |
| 2.9.2 | Pre-Operational Tests | 53 |
| 2.9.3 | Operational Tests | 54 |
| 2.9.4 | Preventive Maintenance Programs | 55 |
| 2.9.5 | Repairs and Maintenance | 56 |
| 2.9.6 | Reviews and Audits | 56 |
| 2.9.7 | Records | 57 |
| 2.10 | Module X: Contingency Response Plans and Procedures | 58 |
| 2.10.1 | Contingency Plan Documentation | 58 |
| 2.10.2 | LLEA | 59 |
| 2.10.3 | Response Procedures | 59 |
| 2.10.4 | Use of Force | 61 |
| 2.10.5 | Alarm Assessment | 61 |
| 2.10.6 | Records | 63 |

1-1-1
10-1

| | |
|---|----|
| 2.11 Module XI: Reporting of Safeguards Events | 64 |
| 2.11.1 Events to be reported within 1 hour of discovery for facilities possessing SNM | 64 |
| 2.11.2 Events to be reported within 1 hour of discovery for facilities possessing SSNM | 64 |
| 2.11.3 Events required to be logged within 24 hours of discovery | 66 |
| 2.11.4 Notification to NRC of 1 hour reportable events | 67 |
| 2.11.5 Report submittal | 68 |
| 2.11.6 Safeguards Event Log | 70 |
| 2.11.7 Records | 70 |
| Appendix Glossary of Terms | 71 |

1. INTRODUCTION

1.1 Purpose

This NUREG presents the primary physical protection requirements, issued by the U.S. Nuclear Regulatory Commission (NRC), under Title 10 of the U.S. Code of Federal Regulations (hereafter, the Code), applicable to unirradiated Categories I, II, and III material at fixed sites (see "Glossary of Terms," the appendix to this NUREG). The requirements are presented in a modular format in relation to the various physical protection functional areas.

This NUREG may be used by NRC staff, licensees, and applicants as a convenient reference document that outlines the primary physical protection requirements for various categories of material.

1.2 Scope of NUREG

This NUREG does not treat all applicable NRC physical protection requirements. In this regard, NRC requires licensees to be familiar with the applicable regulations of the Code and not limit their designs for physical protection to the scope of this NUREG. Major provisions of the Code that are part of this NUREG include the principal applicable portions of 10 CFR Part 73, "Physical Protection of Plants and Material" (i.e., 10 CFR 73.1; 73.20; 73.45; 73.46; 73.67; 73.70; and 73.71) and Appendix G, "Reportable Safeguards Events." Depending on the category of material under consideration, other parts of the Code that may apply, but are not explicitly within the scope of this document, include the following applicable appendices to Part 73- Appendix B, "General Criteria for Security Personnel;" Appendix C, "Licensee Safeguards Contingency Plans;" and Appendix H, "Minimum Day Firing Criteria;" -- 10 CFR Part 11, "Criteria and Procedures for Determining Eligibility for Access to Special Nuclear Material;" and 10 CFR Part 26, "Fitness for Duty Programs." Further, this document does not address physical protection requirements for spent fuel. These requirements are found under 10 CFR 72.212, for a general license, and 10 CFR 73.51, for a specific license.

1.3 Additional Guidance

A compilation of physical protection guidance, published by NRC and presented under modular groupings as presented in this NUREG, is found in NUREG/BR -0252, "User's Guide to NRC-Published Physical Protection Documents," August 1998.

1.4 Modular Format

The modular format of this NUREG is one that NRC is adopting in the fuel cycle physical protection area, to streamline, and make more user-friendly, its guidance documents.

1.5 Description of NUREG

This NUREG is divided into eleven major modules that represent, in combination, the basic elements of the required physical protection system for Categories I, II, and III material. These modules are as follows:

- Module I: General Requirements
- Module II: General Performance Objectives and Capabilities
- Module III: Threat and Protection Goal
- Module IV: Security Organization
- Module V: Barriers and Designated Areas
- Module VI: Access Control Subsystems and Procedures
- Module VII: Detection, Surveillance, and Alarm Subsystems
- Module VIII: Communications Subsystems
- Module IX: Test and Maintenance Program for Physical Protection Equipment
- Module X: Contingency Response Plans and Procedures
- Module XI: Reporting of Safeguards Events

For each module, listed are the requirements that a licensee must meet in designing its physical protection system. A regulatory reference is included with each requirement.

2. PHYSICAL PROTECTION PLAN COMPONENT MODULE

2.1 Module I : General Requirements

| Component | Category I | Category II | Category III |
|---------------------------------|---|--|---|
| 2.1.1 Physical Protection Plans | <p>Each applicant for a license to possess or use, at any site or contiguous sites subject to licensee control, a formula quantity of strategic special nuclear material (SSNM), must include a physical protection plan. This plan must describe how the applicant will meet the applicable requirements of 10 CFR Part 73.</p> <p style="text-align: center;">§ 70.22(h)(1)</p> | <p>Each licensee who possesses or uses special nuclear material (SNM) of moderate strategic significance must submit a physical protection plan or an amended physical protection plan describing how the licensee will comply with all the requirements of paragraph (d) of § 73.67.</p> <p style="text-align: center;">§ 73.67(c)(1)</p> | <p>Each licensee who possesses or uses 10 kg or more of SNM of low strategic significance must submit a physical protection plan or an amended physical protection plan describing how the licensee will comply with all the requirements of paragraph (f) of § 73.67.</p> <p style="text-align: center;">§ 73.67(c)(1)</p> |
| 2.1.2 Implementation | <p>If a future revision to the regulations dictates the need for an implementation schedule, then this schedule will either be identified in the regulations or developed on a site-specific basis.</p> | <p>Within 30 days after the plan submitted pursuant to paragraph (c)(1) of §73.67 is approved, or when specified by the U.S. Nuclear Regulatory Commission (NRC) in writing, it must be implemented.</p> <p style="text-align: center;">§73.67(c)(2)</p> | <p>Within 30 days after the plan submitted pursuant to paragraph (c)(1) of §73.67 is approved, or when specified by NRC in writing, it must be implemented.</p> <p style="text-align: center;">§73.67(c)(2)</p> |

2.1 Module 1: General Requirements (cont.)

| Component | Category I | Category II | Category III |
|---------------|--|--|--|
| 2.1.3 Records | <p>The licensee must retain a copy of the physical protection plan and each change to the plan as a record for a period of 3 years following the date on which the licensee last possessed the appropriate type and quantity of SNM requiring this record.</p> <p>Each record required by Part 73 must be legible throughout the retention period specified by each Commission regulation.</p> <p>The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period.</p> <p>The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period.</p> | <p>The licensee must retain a copy of the effective physical protection plan as a record for 3 years after the licensee possesses the SNM. Copies of superseded material must be retained for 3 years after each change.</p> <p>Each record required by Part 73 must be legible throughout the retention period specified by each Commission regulation.</p> <p>The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period.</p> <p>The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period.</p> | <p>The licensee must retain a copy of the effective physical protection plan as a record for 3 years after the licensee possesses the SNM. Copies of superseded material must be retained for 3 years after each change.</p> <p>Each record required by Part 73 must be legible throughout the retention period specified by each Commission regulation.</p> <p>The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period.</p> <p>The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period.</p> |

2.1 Module 1: General Requirements (cont.)

| Component | Category I | Category II | Category III |
|-----------------------|--|---|---|
| 2.1.3 Records (cont) | <p>Records such as letters, drawings, and specifications, must include all pertinent information such as stamps, initials, and signatures.</p> <p>The licensee must maintain adequate safeguards against tampering with and loss of records.</p> <p>In addition, the following records must be kept for licensees subject to the provisions of 10 CFR 73.20, 73.45, and 73.46:</p> <p>Names and addresses of all individuals who have been designated as authorized individuals. The licensee must retain this record of currently designated authorized individuals for the period during which the licensee possesses the appropriate type and quantity of SNM and for 3 years thereafter. Copies of superseded material must be retained for 3 years after each change.</p> <p>§70.22(h)(2) & 73.70 (a)</p> | <p>Records such as letters, drawings, and specifications, must include all pertinent information such as stamps, initials, and signatures.</p> <p>The licensee must maintain adequate safeguards against tampering with and loss of records.</p> <p>§73.67(c)(1) and 73.70(a)</p> | <p>Records such as letters, drawings, and specifications, must include all pertinent information such as stamps, initials, and signatures.</p> <p>The licensee must maintain adequate safeguards against tampering with and loss of records.</p> <p>§73.67(c)(1) and 73.70(a)</p> |

2.2 Module II: General Performance Objectives and Capabilities

| Component | Category I | Category II | Category III |
|--------------------------------|---|--|---|
| 2.2.1 Performance Objectives | <p>Each licensee authorized to possess or use formula quantities of SSNM at any site or contiguous sites must establish and maintain or make arrangements for a physical protection system that will provide high assurance that activities involving SNM are not inimical to the common defense and security, and do not constitute an unreasonable risk to the public health and safety.</p> <p>§73.20(a)</p> | <p>Each licensee authorized to possess or use SNM of moderate strategic significance must establish and maintain a physical protection system that will: (1) minimize the possibilities for unauthorized removal of SNM consistent with the potential consequences of such actions; and (2) facilitate the location and recovery of missing SNM.</p> <p>§73.67(a)(1)</p> | <p>Each licensee authorized to possess or use SNM of low strategic significance must establish and maintain a physical protection system that will: (1) minimize the possibilities for unauthorized removal of SNM consistent with the potential consequences of such actions; and (2) facilitate the location and recovery of missing SNM.</p> <p>§73.67(a)(1)</p> |
| 2.2.2 Performance Capabilities | <p>To meet the general performance objective of paragraph 73.20 the physical protection system must:</p> <p>Provide for the following performance capabilities described in §73.45:</p> <p>(b)(1) detect attempts to gain unauthorized access or introduce unauthorized material across material access or vital area boundaries by stealth or force;</p> | <p>To meet the general performance objectives of paragraph 73.67(a) the physical protection system must provide:</p> <p>(l) early detection and assessment of unauthorized access or activities by an external adversary within the controlled access area containing SNM;</p> | <p>To meet the general performance objectives of paragraph 73.67(a) the physical protection system must provide:</p> <p>(l) early detection and assessment of unauthorized access or activities by an external adversary within the controlled access area containing SNM;</p> |

2.2 Module II: General Performance Objectives and Capabilities (cont.)

| Component | Category I | Category II | Category III |
|--|---|---|--|
| 2.2.2 Performance Capabilities (cont.) | (2) detect attempts to gain unauthorized access or introduce unauthorized materials into material access areas or vital areas by deceit ; (c)(1) detect unauthorized activities or conditions within protected areas, material access areas, and vital areas; (d)(1) detect unauthorized placement and movement of SSNM within the material access area; (e)(1) detect attempts at unauthorized removal of SSNM from material access areas by stealth or force; (2) confirm the identity and quantity of SSNM presented for removal from a material access area and detect attempts at unauthorized removal of SSNM from material access areas by deceit; (f)(1) detect attempts to gain unauthorized access or introduce unauthorized persons, vehicles, or materials into the protected area (PA) by stealth or force; (2) detect attempts to gain unauthorized access or introduce unauthorized persons, vehicles, or materials into the PA by deceit; and, (g) a response capability must also be provided. | (ii) early detection of removal of SNM by an external adversary from a controlled access area; (iii) assure proper placement and transfer of custody of SNM; and (iv) respond to indications of an unauthorized removal of SNM and then notify the appropriate response forces of its removal to facilitate its recovery. §73.67(a)(2) | (ii) early detection of removal of SNM by an external adversary from a controlled access area; (iii) assure proper placement and transfer of custody of SNM; and (iv) respond to indications of an unauthorized removal of SNM and then notify the appropriate response forces of its removal, to facilitate its recovery. §73.67(a)(2) |

2.2 Module II: General Performance Objectives and Capabilities (cont.)

| Component | Category I | Category II | Category III |
|--|--|-------------|--------------|
| 2.2.2 Performance Capabilities (cont.) | <p>In addition, the physical protection system must:</p> <p>Be designed with sufficient redundancy and diversity;</p> <p>Include a safeguards contingency capability;</p> <p>Include a testing and maintenance program; and</p> <p>Establish, maintain, and follow NRC-approved safeguards physical protection and safeguards contingency plans that describe how the licensee will comply with the requirements of paragraphs (a) and (b) of §73.20.</p> <p>§73.20 (b)(1-5) and 73.45 (a)-(g)</p> | | |

2.3 Module III: Threat and Protection Goal

| Component | Category I | Category II | Category III |
|---|--|---|--|
| <p>2.3.1 Threat and Protection Goal</p> | <p>A physical protection system must be designed to protect against the following design basis threat for theft or diversion of formula quantities of SSNM:</p> <p>(i) a determined, violent, external assault, attack by stealth, or deceptive actions by a small group with the following attributes, assistance, and equipment:</p> <p>(a) well-trained, including military training and skills, and dedicated individuals;</p> <p>(b) inside assistance that may include a knowledgeable individual who attempts to participate in a passive role (e. g., provide information); an active role (e.g. facilitate entrance and exit, disable alarms and communications, participate in a violent attack); or both;</p> | <p>The effective amendments in 10 CFR 73.67 have been primarily designed to require early detection of theft of SNM of moderate strategic significance.</p> <p>44FR43280 Statement of Considerations, "Safeguards Requirements for Special Nuclear Material of Moderate and Low Strategic Significance"</p> | <p>The effective amendments in 10 CFR 73.67 have been primarily designed to require early detection of theft of SNM of low strategic significance.</p> <p>44FR43280 Statement of Considerations, "Safeguards Requirements for Special Nuclear Material of Moderate and Low Strategic Significance"</p> |

2.3 Module III: Threat and Protection Goal (cont.)

| Component | Category I | Category II | Category III |
|--|---|-------------|--------------|
| 2.3.1 Threat and Protection Goal (cont.) | <p>(c) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers, and having effective long-range accuracy.</p> <p>(d) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system;</p> <p>(e) land vehicles used for transporting personnel and their hand-carried equipment; and</p> <p>(f) the ability to operate as two or more teams:</p> <p>(ii) an individual, including an employee (in any position), and</p> <p>(iii) a conspiracy between individuals in any position who may have: (A) access to and detailed knowledge of nuclear power plants or the facilities referred to in paragraph 73.20(a), or (B) items that could facilitate theft of special nuclear material (e.g., small tools, substitute material, false documents, etc.), or both.</p> <p>§73.1(a)(2)(a-f)</p> | | |

2.4 Module IV: Security Organization

| Component | Category I | Category II | Category III |
|---|---|---|---|
| <p>2.4.1 Establishment of Security Organization</p> | <p>A security organization with guards must be established. If a contract guard force is used for site security, the licensee's written agreement with the contractor must clearly show:</p> <ul style="list-style-type: none"> (i) the licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan; (ii) NRC may inspect, copy, and take away copies of all reports and documents required to be kept by Commission regulations, orders, or applicable license conditions, whether such reports and documents are kept by the licensee or the contractor; (iii) the requirement in §73.46(b)(4), that the licensee demonstrate the ability of physical security personnel to perform their assigned duties and responsibilities, include demonstration of the ability of the contractor's physical security personnel to perform their assigned duties and responsibilities in carrying out the provisions of the security plan and these regulations; and, | <p>A security organization must be established or the current organization modified to consist of at least one watchman per shift who is able to assess and respond to any unauthorized penetrations or activities in the controlled access areas.</p> <p style="text-align: right;">§73.67(d)(8)</p> | <p>The licensee must assure that a watchman or offsite response force will respond to all unauthorized penetrations or activities.</p> <p style="text-align: right;">§73.67(f)(3)</p> |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|--|--|---|--|
| 2.4.1 Establishment of Security Organization (cont.) | (iv) the contractor will not assign any personnel to the site who have not first been made aware of these responsibilities. §73.46(b)(1) | | |
| 2.4.2 Response Force | <p>A Tactical Response Team consisting of a minimum of 5 members must be available at the facility to fulfill assessment and response requirements.</p> <p>A force of guards or armed response personnel must be available to provide assistance as necessary in addition to the Tactical Response Team.</p> <p>The size and availability of the additional force must be determined on the basis of site-specific considerations that could affect the ability of the total onsite response force to engage and impede the adversary force until offsite assistance arrives.</p> <p>The rationale for the total number and availability of onsite armed response personnel must be included in the physical protection plans.</p> <p>§73.46(h)(3)</p> | <p>One watchman per shift must be able to assess and respond to any unauthorized penetrations or activities in the controlled access areas.</p> <p>§73.67(d)(8)</p> | <p>A watchman or offsite response force must respond to all unauthorized penetrations or activities.</p> <p>§73.67(f)(3)</p> |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|---|---|---|
| <p>2.4.3 Security Organization Management</p> | <p>At least one full- time member of the security organization with the authority to direct the physical protection activities of the security organization must be onsite at all times.</p> <p>A management system must be in place that will provide for the development, revision, implementation, and enforcement of security procedures. The system must include:</p> <p>(I) written security procedures that document the structure of the security organization and detail the duties of all individuals responsible for security; and</p> <p>(ii) provisions for written approval of security procedures, and any revisions thereto, by the individual with overall responsibility for the security function, must be maintained.</p> <p>§73.46(b)(2)&(3)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for a security organization management system.</p> | <p>Under the provisions in Part 73, there are no explicit requirements for a security organization management system.</p> |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|--|--|---|--|
| <p>2.4.4 Qualifications for Employment in Security</p> | <p>An individual must not be permitted to act as a Tactical Response Team member, armed response person, guard, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security duty in accordance with Appendix B, Part 73, "General Criteria for Security Personnel." The ability of the physical security personnel, whether licensee or contractor employees, to carry out their assigned duties and responsibilities, must be demonstrated on the request of an authorized member of the Commission.</p> <p>Within any given period of time, a member of the security organization may not be assigned to, or have direct operational control over, more than one of the redundant elements of a physical protection subsystem if such assignment or control could result in the loss of effectiveness of the subsystem.</p> <p>New employees, hired after the approval date, must meet or exceed qualification criteria before assignments as Tactical Response Team members, armed response personnel, or guards.</p> <p>In addition to the above requirements, refer to Appendix B I. A & B to Part 73.</p> <p>§73.46(b)(4)(5)&(11)</p> | <p>See Appendix B, Part 73, sections IA.,(1)(a)(b), and B (1)(a).</p> | <p>See Appendix B, Part 73, sections IA., (1)(a)(b), and B (1)(a).</p> |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|----------------------------|---|---|---|
| 2.4.5 Guard Force Training | <p>Tactical Response Team members, armed response personnel, and guards must be trained, equipped, and qualified to perform each assigned security duty in accordance with Appendix B, Part 73. In addition, Tactical Response Team members, armed response personnel, and guards must be trained, equipped, and qualified for use of their assigned weapons in accordance with paragraphs (b)(6) and (b)(7) of § 73.46.</p> <p>Tactical Response Team members, armed response personnel, and guards must be trained, and qualified in accordance with the physical fitness testing requirements in either paragraphs (b)10 and (b)(11) or (b)(12) of § 73.46.</p> <p>Each Tactical Response Team member, armed response person, and guard, whether a licensee or contractor employee, must requalify in accordance with Appendix B, Part 73.</p> <p>Tactical Response Team members, armed response persons, and guards must also requalify with day and night firing in accordance with paragraph (b)(7) of § 73.46 at least once every 12 months.</p> | See Appendix B, Part 73, applicable sections of II. | See Appendix B, Part 73, applicable sections of II. |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|------------------------------------|--|-------------|--------------|
| 2.4.5 Guard Force Training (cont.) | <p>In addition to the weapons qualification and requalification criteria of Appendix B, Part 73, Tactical Response Team members, armed response persons, and guards must qualify and requalify, at least every 12 months, for day and night firing, with assigned weapons, in accordance with Appendix H, Part 73, "Minimum Day Firing Criteria."</p> <p>Tactical Response Team members, armed response persons, and guards will be allowed to practice-fire before qualification and requalification, but will only be given one opportunity to fire for record on the same calendar day.</p> <p>If a Tactical Response Team member, armed response person, or guard fails to qualify or requalify, he/she must be removed from security duties that require the use of firearms, and the individual must be retrained before any subsequent attempt to qualify or requalify.</p> <p>If an individual fails to qualify or requalify on two successive attempts, he/she must receive additional training and successfully fire two consecutive qualifying scores before being reassigned to armed security duties.</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|------------------------------------|---|--|--|
| 2.4.5 Guard Force Training (cont.) | <p>In addition, Tactical Response Team members, armed response personnel, and guards must be prepared to demonstrate day and night firing qualification with their assigned weapons at any time, on request by an authorized NRC representative.</p> <p>In addition to the training requirements contained in Appendix B, Part 73, Tactical Response Team members must successfully complete training in response tactics.</p> <p>§73.46(b)(4),(7)&(8)</p> | | |
| 2.4.6 Physical Fitness Testing | <p>In addition to the medical examinations and physical fitness requirements of paragraph I.C of Appendix B, Part 73, each Tactical Response Team member, armed response person, and guard, except as provided in paragraph (b)(10)(v) of § 73.46 , must participate in a physical fitness training program on a continuing basis.</p> <p>The elements of the physical fitness training program must include, but not necessarily be limited to, the following:</p> | Under the provisions in Part 73, physical fitness testing is not required. | Under the provisions in Part 73, physical fitness testing is not required. |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|---|-------------|--------------|
| <p>2.4.6 Physical Fitness Testing (cont.)</p> | <p>(a) Training sessions of sufficient frequency, duration, and intensity to be of aerobic benefit, (e.g., normally a frequency of 3 times per week, maintaining an intensity of approximately 75 percent of maximum heart rate for 20 minutes);</p> <p>(b) Activities that use large muscle groups, that can be maintained continuously, and that are rhythmical and aerobic in nature (e.g., running, bicycling, rowing, swimming, or cross-country skiing); and</p> <p>(c) Musculoskeletal training exercises that develop strength, flexibility, and endurance in the major muscle groups, (e.g., legs, arms, and shoulders).</p> <p>Tactical Response Team members, armed response personnel, and guards must be assessed for general fitness once every 4 months to determine the effectiveness of the continuing physical fitness training program.</p> <p>Individual exercise programs must be modified to be consistent with the needs of each participating Tactical Response Team member, armed response person, and guard, and consistent with the environments in which they must be prepared to perform their duties.</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|---|-------------|--------------|
| <p>2.4.6 Physical Fitness Testing (cont.)</p> | <p>Assessments must include a recent health history, measures of cardiovascular fitness, percent of body fat, flexibility, muscular strength, and endurance.</p> <p>Individuals who exceed 4 months without being assessed for general fitness, because of excused time off from work, must be assessed within 15 calendar days of returning to duty as Tactical Response Team members, armed response persons, or guards.</p> <p>Licensees may temporarily waive an individual's participation in the physical fitness training program on the advice of the licensee's examining physician, during which time the individual may not be assigned duties as a Tactical Response Team member.</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|---|-------------|--------------|
| <p>2.4.6 Physical Fitness Testing (cont.)</p> | <p>Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the physical fitness training program specified in paragraph (b)(10) of § 73.46, provided that they are not assigned temporary response guard duties.</p> <p>In addition to the physical fitness demonstration contained in paragraph I.C of Appendix B, Part 73, Tactical Response Team members, armed response persons, and guards must meet or exceed the annual performance testing requirements in paragraphs (b)(11)(I) through (b)(11)(v) of §73.46, except as provided in paragraph (b)(11)(vi) of § 73.46, initially and at least once every 12 months thereafter.</p> <p>For Tactical Response Team members the criteria are a (1-mile) run in 8 minutes and 30 seconds or less, and a (40-yard) dash starting from a prone position in 8 seconds or less.</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|---|-------------|--------------|
| <p>2.4.6 Physical Fitness Testing (cont.)</p> | <p>For armed response personnel and guards who are not members of the Tactical Response Team, the criteria are a (½ mile) run in 4 minutes and 40 seconds or less, and a (40- yard) dash starting from the prone position in 8.5 seconds or less.</p> <p>The test may be taken in ordinary athletic attire under the supervision of licensee designated personnel.</p> <p>Incumbent Tactical Response Team members, armed response personnel, and guards must meet or exceed the qualification criteria within 12 months of NRC approval of the licensee's revised physical protection plan.</p> <p>Tactical Response Team members, armed response personnel, and guards who do not meet or exceed the qualification criteria, must be placed in a monitored remedial physical fitness training program and they must be relieved from their security duties until they satisfactorily meet or exceed the qualification criteria.</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|--|-------------|--------------|
| <p>2.4.6 Physical Fitness Testing (cont.)</p> | <p>The annual performance testing for an individual may be temporarily waived on the advice of the licensee's examining physician, during which time the individual may not be assigned duties as a Tactical Response Team member.</p> <p>Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the annual performance testing specified in paragraph (b)(11) of §73.46, provided that they are not assigned temporary response guard duties.</p> <p>The licensee may elect to comply with the physical fitness testing requirements of §73.46(b)(10) and (b)(11) or (b)(12) as follows:</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|--|-------------|--------------|
| <p>2.4.6 Physical Fitness Testing (cont.)</p> | <p>In addition to the physical fitness qualifications of paragraph I.C. of Appendix B, Part 73, each licensee subject to the requirements of §73.46 must develop and submit to NRC, for approval, site-specific, content-based, physical fitness performance tests that when administered to each Tactical Response Team member, armed response personnel, or guard, will duplicate the response duties these individuals may need to perform during a strenuous tactical engagement.</p> <p>The test must be administered to each Tactical Response Team member, armed response personnel, and guard once every 3 months.</p> <p>The test must specifically address the physical capabilities needed by armed response personnel during a strenuous tactical engagement at the licensed facility.</p> <p>Individuals who exceed 3 months without having been administered the test, because of excused time off from work, must be tested within 15 calendar days of returning to duty as Tactical Response Team members, armed response persons, or guards</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|--|--|---|---|
| 2.4.6 Physical Fitness Testing (cont.) | <p>Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the performance test specified in paragraph (b)(12) of §73.46 provided they are not assigned temporary response guard duties.</p> <p>§73.46(b)(10),(11)&(12)</p> | | |
| 2.4.7 Fitness for Duty Programs (FFD) | <p>Each licensee authorized to possess or use formula quantities of SSNM must implement an FFD program that complies with 10 CFR Part 26.</p> <p>Refer to Part 26</p> | Under the provisions in Part 26, an FFD program is not required. | Under the provisions in Part 26, an FFD program is not required. |
| 2.4.8 Medical Requirements | <p>Within 30 days before participation in the physical fitness training program, each Tactical Response Team member, armed response person, and guard, must be given a medical examination, including a determination and written certification, by a licensed physician, that there are no medical contraindications, as disclosed by the medical examination, to participation in the physical fitness performance test.</p> | Under the provisions in 10 CFR Part 73, physical fitness testing and medical examinations are not required. However, refer to section 2.4.4 above, "Qualifications for Employment in Security." | Under the provisions in 10 CFR Part 73, physical fitness testing and medical examinations are not required. However, refer to section 2.4.4 above, "Qualifications for Employment in Security." |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---|--|-------------|--------------|
| <p>2.4.8 Medical Requirements (cont.)</p> | <p>Within 30 days before the first administration of the physical fitness performance tests, and on an annual basis thereafter, Tactical Response Team members, armed response personnel, and guards must be given medical examinations, including determinations and written certifications by a licensed physician, that there are no medical contraindications, as disclosed by the medical examinations, to participation in the physical fitness performance tests.</p> <p>In addition to the aforementioned medical requirements, refer to Appendix B, I.C Part 73.</p> <p>§73.46(b)(10),(11)&(12)</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|---------------------------------|---|---|---|
| 2.4.9 Security Force Armament | <p>Each guard must be armed with a handgun, as described in Appendix B, Part 73.</p> <p>Each Tactical Response Team member must be armed with a 9-mm semiautomatic pistol.</p> <p>All but one member of the Tactical Response Team must be additionally armed with either a shotgun or a semiautomatic rifle, as described in Appendix B, Part 73. The remaining member of the Tactical Response Team must carry, as an individually assigned weapon, a rifle of no less caliber than 7.62 mm (.30 inches).</p> <p>§73.46(b)(6)</p> | Under the provisions in Part 73, support equipment for watchman is not explicitly required. | Under the provisions in Part 73, support equipment for watchman is not explicitly required. |
| 2.4.10 Force-on-Force Exercises | Tactical Response Team and guard exercises must be conducted to demonstrate: overall security system effectiveness; the ability of the security force to perform response and contingency plan responsibilities; and individual skills in assigned team duties. | Under the provisions in Part 73, force-on-force exercises are not required. | Under the provisions in Part 73, force-on-force exercises are not required. |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|--|---|-------------|--------------|
| <p>2.4.10 Force-on-Force Exercises (cont.)</p> | <p>During the first 12- month period following the date specified in paragraph (1)(2)(ii) of §73.46(b), an exercise must be carried out at least every 3 months for each shift, half of which are to be force-on-force. Subsequently, during each 12-month period, commencing on the anniversary of the date specified in paragraph (1)(2)(ii) of §73.46 (b), an exercise must be carried out at least every 4 months for each shift, one third of which are to be force-on-force.</p> <p>These exercises will be used by the licensee to demonstrate the capability to respond to attempts to steal SSNM.</p> <p>During each 12-month period, NRC must observe one of the force-on-force exercises.</p> <p>NRC must be notified of the aforementioned scheduled exercise 60 days before that exercise.</p> <p>§73.46(b)(9)</p> | | |

2.4 Module IV: Security Organization (cont.)

| Component | Category I | Category II | Category III |
|----------------|---|--|--|
| 2.4.11 Records | <p>A copy of the current written security procedures must be retained as a record until the Commission terminates the license for which these procedures were developed, and if any portion of these procedures are superseded, retain the superseded material for 3 years after the change.</p> <p>The results of qualification and requalification for security force members must be documented and retained as a record for 3 years after each qualification and requalification. The results of weapons qualification and requalification for day and night firing must be documented and retained as a record for 3 years after each qualification and requalification.</p> <p>The completion of training in response tactics for members of the Tactical Response Team must be documented and retained as a record for 3 years after training is completed.</p> <p>The results of each force on force exercise must be documented and retained for 3 years after each exercise is completed.</p> <p>A record of each individual's physical fitness performance testing must be retained for 3 years.</p> <p>§73.46(b)(3),(4),(7),(8),(9),&(11)</p> | See Appendix B, Part 73, applicable portions of section I.F. | See Appendix B, Part 73, applicable portions of section I.F. |

2.5 Module V: Barriers and Designated Areas

| Component | Category I | Category II | Category III |
|--|---|--|--|
| <p>2.5.1 Protected and Controlled Access Area Barriers</p> | <p>Perimeter of PA must have two separate physical barriers with an intrusion detection system placed between them.</p> <p>The inner barrier must be positioned and constructed to enhance assessment of penetration attempts and to delay attempts at unauthorized exit from PA.</p> <p>Physical barriers at the perimeter of the PA must be separated from any other barrier designated as a physical barrier for a vital area or material access area (MAA) within the PA.</p> <p>§73.46(c)(1)&(2)</p> | <p>Store the material only within a controlled access area such as a vault-type room, or approved security cabinet, or equivalent, that is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.</p> <p>§73.67(d)(2)</p> | <p>Store or use material only within a controlled access area.</p> <p>§73.67(f)(1)</p> |
| <p>2.5.2 Vehicle Barriers</p> | <p>Perimeter of PA must incorporate features and structures that prevent forcible vehicle entry.</p> <p>§73.46(c)(1)</p> | <p>Under the provisions in Part 73, vehicle barriers are not required.</p> | <p>Under the provisions in Part 73, vehicle barriers are not required.</p> |

2.5 Module V: Barriers and Designated Areas (cont.)

| Component | Category I | Category II | Category III |
|---|--|---|---|
| <p>2.5.3 Material and Controlled Access Area Barriers</p> | <p>Vital equipment must be located only within a vital area, and SSNM must be stored or processed only in an MAA.</p> <p>Both vital areas and MAAs must be located within a PA so that access to vital equipment and SSNM requires passage through at least three physical barriers.</p> <p>§73.46(c)(1)</p> | <p>Store the material only within a controlled access area such as a vault-type room or approved security cabinet or equivalent that is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.</p> <p>§73.67(d)(2)</p> | <p>Store or use material only within a controlled access area.</p> <p>§73.67(f)(1)</p> |
| <p>2.5.4 Isolation Zones</p> | <p>Isolation zones must be maintained in outside areas adjacent to the physical barrier at the perimeter of the PA.</p> <p>Isolation zones must be large enough to permit observation of the activities of people on either side of the barrier in the event of penetration.</p> <p>If parking facilities are provided for employees or visitors, they must be located outside of the isolation zone and exterior to the PA.</p> <p>§73.46(c)(3)</p> | <p>Under the provisions in Part 73, PAs or associated isolation zones are not required.</p> | <p>Under the provisions in Part 73, PAs or associated isolation zones are not required.</p> |

2.5 Module V: Barriers and Designated Areas (cont.)

| Component | Category I | Category II | Category III |
|-----------------------------------|--|---|--|
| 2.5.5 Illumination | <p>Isolation zones and all exterior areas within the PA must be provided with illumination sufficient for monitoring and observing requirements of paragraphs (c)(3), (e)(8), (h)(4), and (h)(6) of §73.46, but not less than 0.2 footcandles measured horizontally at ground level.</p> <p>§73.46(c)(4)</p> | <p>Use material only within a controlled access area that is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.</p> <p>§73.67(d)(1)</p> | <p>Under the provisions of Part 73, there are no requirements for illumination of the controlled access areas.</p> |
| 2.5.6 Storage of Nuclear Material | <p>SSNM, other than alloys, fuel elements, or fuel assemblies, must: (l) be stored in a vault when not undergoing processing if the material can be used directly in the manufacture of a nuclear explosive device.</p> <p>Vaults used to protect SSNM that can be used in the manufacture of a nuclear explosive must be designed to prevent entry to stored SSNM by a single action in a forced entry attempt. Except as such single action would both destroy the barrier and render contained SSNM incapable of being removed, and must provide sufficient delay to prevent removal of stored SSNM before arrival of response personnel capable of neutralizing the design basis threat stated in §73.1.</p> | <p>Store the material only within a controlled access area such as a vault-type room or approved security cabinet or equivalent, which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.</p> <p>§73.67(d)(2)</p> | <p>Store or use material only within a controlled access area.</p> <p>§73.67(f)(1)</p> |

2.5 Module V: Barriers and Designated Areas (cont.)

| Component | Category I | Category II | Category III |
|--|--|-------------|--------------|
| <p>2.5.6 Storage of Nuclear Material (cont.)</p> | <p>SSNM must be stored in tamper-indicating containers.</p> <p>SSNM must be processed in MAAs with barriers that provide significant delay to penetration.</p> <p>SSNM must be kept in locked compartments or locked process equipment while undergoing processing, except when personally attended.</p> <p>More than one vital area or MAA may be located within a single PA.</p> <p>§73.46(c)(1)&(5)</p> | | |

2.5 Module V: Barriers and Designated Areas (cont.)

| Component | Category I | Category II | Category III |
|--|--|--|---|
| <p>2.5.7 Storage of Enriched Uranium Scrap</p> | <p>Enriched uranium scrap (enriched to 20 percent or greater) in the form of small pieces, cuttings, chips, solutions, or in other forms resulting from a manufacturing process, contained in (30-gallon) or larger containers with a uranium-235 content of less than 0.25 grams per liter, may be stored within a locked and separately fenced area within a larger PA, provided the storage area fence is no closer than (25 feet) to perimeter of PA</p> <p>The storage area, when unoccupied, must be protected by a patrolling guard or watchman at intervals not exceeding 4 hours, or by intrusion alarms.</p> <p>§73.46(c)(6)</p> | <p>Category II requirements, under 10 CFR 73.67, do not provide separate requirements for material in the form of scrap.</p> | <p>Category III requirements, under 10 CFR 73.67, do not provide separate requirements for material in the form of scrap.</p> |

2.6 Module VI: Access Control Subsystems and Procedures

| Component | Category I | Category II | Category III |
|--|---|---|--|
| <p>2.6.1 Numbered Picture Badge System</p> | <p>A numbered picture badge identification subsystem must be used for all individuals who are authorized access to PA without escort.</p> <p>Individuals not employed by the licensee, but who require frequent and extended access to PAs, MAAs, or vital areas may be authorized access to such areas without escort provided he/she receives a picture badge on entrance into the PA, and returns the badge on exiting from the PA. The badge must indicate non-employee, no-escort-required, areas to which access is authorized, and the period for which access has been authorized.</p> <p>The badges must be displayed by all individuals while inside the PA.</p> <p>Specially coded numbered badges must be issued to individuals authorized unescorted access to vital areas, MAAs, and controlled access areas. The vital areas, MAA, and controlled access areas to which access is authorized must also be indicated.</p> <p>§73.46(d)(1)&(2)</p> | <p>Develop and maintain a controlled badging system, to identify and limit access to the controlled access areas to authorized individuals.</p> <p>§73.67(d)(5)</p> | <p>Under the provisions in Part 73, a numbered picture badge system is not required.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|--|---|---|---|
| <p>2.6.2 Access to Material and Controlled Access Areas</p> | <p>Unescorted access to vital areas, MAAs, and controlled access areas must be limited to individuals who are authorized access to the material and equipment in such areas and who require such access to perform their duties.</p> <p>Access to MAAs must include at least two individuals.</p> <p>No activities other than those that require access to SSNM or to equipment used in processing, use, or storage of SSNM, or necessary maintenance, will be permitted within an MAA.</p> <p>§73.46(d)(2)</p> | <p>Limit access to the controlled access areas to authorized or escorted individuals who require such access to perform their duties.</p> <p>§73.67(d)(6)</p> | <p>By definition, a controlled access area is any temporary or permanently established area that is clearly demarcated, access to which is controlled, and that affords isolation of the material or person within it.</p> <p>§73.2</p> |
| <p>2.6.3 Access Controls at the PA for:</p> <p>2.6.3.1 Personnel</p> | <p>Written procedures must be established and followed that will permit access control personnel to identify those vehicles that are authorized and those materials that are not authorized entry to the PAs and MAAs.</p> <p>All points of personnel access into a PA must be controlled. All individuals entering the PA must be identified, searched for firearms, explosives, and incendiary devices; and the individuals' authorizations must be checked. Federal, State, and local law enforcement personnel on official duty and US Department of Energy (DOE) couriers engaged in the transport of SSNM are exempt.</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.1 of this NUREG.</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.1 of this NUREG.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|--|---|-------------|--------------|
| <p>2.6.3 (cont.) Access Controls at the PA for:</p> <p>2.6.3.1 Personnel (cont.)</p> | <p>The search function for detection of firearms, explosives, and incendiary devices must be accomplished through the use of detection equipment capable of detecting both firearms and explosives.</p> <p>The individual responsible for the last access control function (controlling admission to the PA) must be isolated within a structure with bullet-resisting walls, doors, ceiling, floor, and windows.</p> <p>Whenever the licensee has cause to suspect that an individual is attempting to introduce firearms, explosives, or incendiary devices into a PA the licensee must conduct a physical pat-down search of that individual.</p> <p>Whenever firearms or explosives detection equipment at a portal is out of service or not operating satisfactorily, a physical pat-down search must be conducted of all persons who would otherwise have been subject to search using the equipment.</p> | | |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|--|---|--|---|
| <p>2.6.3 (cont.) Access Controls at the PA for:</p> <p>2.6.3.1 Personnel (cont.)</p> | <p>Licensees may not announce nor otherwise communicate to their employees or site contractors the arrival or presence of an NRC safeguards inspectors unless specifically requested to do so by the NRC safeguards inspectors.</p> <p>§73.46(d)(3),(4)&(15)</p> | | |
| <p>2.6.3 (cont.) Access Controls at the PA for:</p> <p>2.6.3.2 Hand-Carried Packages</p> | <p>At the point of personnel and vehicle access into a PA all hand-carried packages must be searched for firearms, explosives, and incendiary devices. Those individuals exempted from search under §73.46(d)(4)(I) are excluded.</p> <p>§73.46(d)(5)</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.2. of this NUREG.</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.2 of this NUREG.</p> |
| <p>2.6.3 (cont.) Access Controls at the PA for:</p> <p>2.6.3.3 Delivered Packages</p> | <p>All packages and materials for delivery into a PA must be checked for proper identification and authorization and searched for firearms, explosives, and incendiary devices before admittance to the PA, except those Commission- approved delivery & inspection activities specifically designated by the licensee to be carried out within MAAs, vital areas, or PAs, for reasons of safety, security, or operational necessity.</p> <p>§73.46(d)(6)</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.2 of this NUREG.</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.2 of this NUREG.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|---|---|---|---|
| <p>2.6.3 (cont.) Access Controls at the PA for:</p> <p>2.6.3.4 Vehicles</p> | <p>Written procedures must be established and followed that will permit access control personnel to identify those vehicles that are authorized entry to protected, material access, and vital areas.</p> <p>All points of vehicle access into the PA must be controlled.</p> <p>All vehicles, except DOE vehicles engaged in transporting SNM, and emergency vehicles under emergency conditions, must be searched for firearms, explosives, and incendiary devices, before entry into the PA.</p> <p>Vehicle areas to be searched include the cab, engine compartment, undercarriage, and cargo area.</p> <p>All vehicles, except designated licensee vehicles, requiring entry into the PA, must be escorted by a member of the security organization while within the PA and, to the extent practicable, must be off-loaded in an area that is not adjacent to a vital area.</p> <p>Designated licensee vehicles must be limited in their use to onsite plant functions and these vehicles must remain in the PA except for operational, maintenance, security, and emergency purposes.</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.3 of this NUREG.</p> | <p>Under the provisions in Part 73, PAs are not required. Refer to section 2.6.4.3 of this NUREG.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|--|--|---|---|
| <p>2.6.3 (cont.) Access Controls at the PA for:</p> <p>2.6.3.4 Vehicles (cont.)</p> | <p>Positive controls must be exercised by the licensee over all designated licensee vehicles, to assure that they are used only by authorized persons and for authorized purposes.</p> <p>§73.46(d)(3),(4),(7)&(8)</p> | | |
| <p>2.6.4 Access Controls at MAAs and Controlled Access Areas for:</p> <p>2.6.4.1 Personnel</p> | <p>All points of personnel access to MAAs, vital areas, and controlled access areas must be controlled.</p> <p>At least two armed guards trained in accordance with §73.46(b)(7) and Appendix B, Part 73, must be posted at each MAA control point, whenever in use.</p> <p>The identification and authorization of personnel at MAA control points must be verified.</p> <p>Each individual exiting a MAA must undergo at least two separate searches for concealed SSNM. For individuals exiting an area that contains only alloyed or encapsulated SSNM, the second search may be conducted in a random manner.</p> <p>§73.46(d)(9)</p> | <p>Conduct screening, before granting an individual unescorted access to the controlled access area where the material is used or stored, so as to obtain information on which to base a decision to permit such access.</p> <p>Assure that all visitors to the controlled access areas are under the constant escort of an individual who has been authorized access to the areas.</p> <p>§73.67(d)(4)&(7)</p> | <p>By definition, a controlled access area is any temporary or permanently established area that is clearly demarcated, access to which is controlled, and that affords isolation of the material or person within it.</p> <p>§73.2</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|---|---|--|---|
| <p>2.6.4 (cont.) Access controls at MAAs and Controlled Access Areas for:</p> <p>2.6.4.2 Packages</p> | <p>Packages must be searched for firearms, explosives, and incendiary devices before entry into a MAA.</p> <p>All material and packages, including trash, wastes, tools, and equipment existing from an MAA must be searched for concealed SSNM by a team of at least two individuals who are not authorized access to that MAA.</p> <p>§73.46(d)(9)</p> | <p>On a random basis, packages leaving the controlled access area must be searched.</p> <p>§73.67(d)(10)</p> | <p>Under the provisions in Part 73, there are no requirements for packages leaving the controlled access area to be searched.</p> |
| <p>2.6.4 (cont.) Access controls at MAAs and Controlled Access Areas for:</p> <p>2.6.4.3 Vehicles</p> | <p>Written procedures must be established and followed that will permit access control personnel to identify those vehicles that are authorized entry into an MAA.</p> <p>All points of vehicle access to MAAs and controlled access areas must be controlled.</p> <p>Identification and authorization of vehicles at the MAA control point must be verified.</p> <p>All vehicles exiting from a MAA must be searched for concealed SSNM by a team of at least two individuals who are not authorized access to that MAA.</p> <p>§73.46(d)(3)&(9)</p> | <p>On a random basis, vehicles leaving the controlled access area must be searched.</p> <p>§73.67(d)(10)</p> | <p>Under the provisions in Part 73 there are no requirements for written procedures to be established to identify or search vehicles.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|---|---|--|---|
| 2.6.5 MAA Exit Search of Contaminated Waste | <p>Before exiting from an MAA, containers of contaminated wastes must be drum-scanned and tamper-sealed by at least two individuals, working and recording their findings as a team, who do not have access to the material processing and storage areas.</p> <p>§73.46(d)(10)</p> | <p>Under the provisions in Part 73, exit searches of contaminated waste are not required.</p> | <p>Under the provisions in Part 73, exit searches of contaminated waste are not required.</p> |
| 2.6.6 Preparing SSNM for Shipment Offsite | <p>SSNM being prepared for shipment offsite, including product, samples, and scraps, must be packed and placed in sealed containers in the presence of at least two individuals working as a team who must verify and certify the content of each shipping container through the witnessing of gross weight measurements and nondestructive assay, and through the inspection of tamper-seal integrity and associated seal records.</p> <p>Areas used for preparing SSNM for shipment and areas used for packaging and screening trash and waste must be controlled access areas, and they must be separated from processing and storage areas.</p> <p>§73.46(d)(11)&(12)</p> | <p>Under the provisions in Part 73, there are no requirements for preparing SSNM for shipment offsite.</p> | <p>By definition, Category III material does not include SSNM.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|--|--|--|---|
| 2.6.7 Escorts and Escorted Individuals | <p>Individuals not permitted by the licensee to enter the PA without escort must be escorted by a watchman or other individual designated by the licensee while in the PA.</p> <p>Individuals requiring escorts must be badged with a badge indicating escort required.</p> <p>Individuals requiring escorts must register, in a log their names, dates, times, purposes of visit, employment affiliations, citizenship, and names of individuals to be visited.</p> <p>§73.46(d)(13)</p> | <p>All visitors to the controlled access areas must be under constant escorts by individuals who have been authorized access to the areas.</p> <p>§73.67(d)(7)</p> | <p>Under the provisions in Part 73, escorts are not required.</p> |
| 2.6.8 Keys, Locks, and Combinations | <p>All keys, locks, combinations, and related equipment used to control access to PAs, MAAs, vital areas, and controlled access areas must be controlled to reduce the probability of compromise. Whenever there is evidence that keys, locks, combinations, and related equipment have been compromised, they must be changed.</p> <p>On termination of employment of an employee, keys, locks, combinations, and related equipment to which that employee had access must be changed.</p> <p>§73.46(d)(14)</p> | <p>Develop and maintain a controlled lock system, to identify and limit access, to the controlled access areas, to authorized individuals.</p> <p>§73.67(d)(5)</p> | <p>Under the provisions in Part 73, controlled lock systems are not required.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|---------------|---|---|--|
| 2.6.9 Records | <p>The procedures that permit access control personnel to identify vehicles that are authorized, and those materials that are not authorized, entry to the PAs, vital areas, and MAAs, must be retained as a record until the Commission terminates each license for which the procedures were developed, and, if any portion is superseded, that material must be retained for 3 years after each change.</p> <p>The records for the findings of drum-scanning and tamper-sealing of containers of contaminated waste exiting from an MAA must be retained for a period of 3 years.</p> <p>The licensee must retain the visitor log as a record for 3 years after the last entry is made in the log.</p> <p>The licensee must maintain the names, addresses, and badge numbers of all individuals authorized to have access to vital equipment or SNM, and the vital areas and MAAs to which authorization is granted. This record must be maintained for the period during which the licensee possesses the appropriate type and quantity of SNM, and for 3 years thereafter.</p> | <p>Records of the controlled badging system must be maintained.</p> <p align="right">§73.67(d)(5)</p> | <p>Under the provisions of 10 CFR Part 73, maintaining access control records is not required.</p> |

2.6 Module VI: Access Control Subsystems and Procedures (cont.)

| Component | Category I | Category II | Category III |
|-----------------------|---|-------------|--------------|
| 2.6.9 Records (cont.) | <p>Copies of superseded material must be maintained for 3 years after each change.</p> <p>The licensee must maintain a register of visitors, vendors, and other individuals not employed by the licensee pursuant to 10 CFR 73.46(d)(13). This register must be retained as a record and made available for inspections, for 3 years after the last entry is made in the register.</p> <p>The licensee must retain procedures for controlling access to PAs and for controlling access to keys for locks used to protect SNM. A copy of the procedures must be retained until the Commission terminates each license for which the procedures were developed, and if any portion of the procedures is superseded, that portion must be retained for 3 years</p> <p>§73.46(d)(3),(10), & (13), and §73.70(b),(c)&(h)</p> | | |

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems

| Component | Category I | Category II | Category III |
|----------------------------------|--|---|---|
| 2.7.1 Isolation Zone Penetration | <p>An intrusion alarm subsystem with a capability to detect penetration through the isolation zone and to permit response action must be provided.</p> <p>§73.46(e)(1)</p> | <p>Under the provisions in Part 73, there are no requirements for isolation zones or PAs. However, controlled access areas must be monitored to detect unauthorized penetrations or activities.</p> <p>§73.67(d)(3)</p> | <p>Under the provisions in Part 73, there are no requirements for isolation zones or PAs. However, controlled access areas must be monitored to detect unauthorized penetrations or activities.</p> <p>§73.67(f)(2)</p> |
| 2.7.2 Emergency Exits | <p>All emergency exits in each PA, MAA, and vital area must be locked to prevent entry from the outside and alarmed to provide local visible and audible alarm annunciation.</p> <p>§73.46(e)(2)</p> | <p>Under the provisions in Part 73, emergency exits are not addressed.</p> | <p>Under the provisions in Part 73, emergency exits are not addressed.</p> |

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems (cont.)

| Component | Category I | Category II | Category III |
|--|--|--|--|
| <p>2.7.3 MAA and Controlled Access Area Protection</p> | <p>Lock and protect, by intrusion alarm, all unoccupied vital areas and MAAs. The intrusion alarm subsystem must alarm on entry of a person anywhere into the area, on exit from the area, and on movement of an individual within the area. With the exception of process material access areas only, the locations of the SSNM within the areas are also required to be alarmed.</p> <p>Vaults and process areas containing SSNM that has not been alloyed nor encapsulated must be monitored by closed circuit television (CCTV) that is monitored in both alarm stations.</p> <p>An individual other than an alarm station operator must be present or have knowledge of access to unoccupied vaults or process areas.</p> <p>The alarm stations must be controlled access areas and their walls, doors, ceilings, floors, and windows must be bullet-resistant.</p> <p>§73.46(e)(3)&(5)</p> | <p>Monitor, with an intrusion alarm or other device or procedures, the controlled access areas, to detect unauthorized penetration or activities.</p> <p>All visitors to the controlled access areas must be under the constant escort of an individual who has been authorized access to the areas.</p> <p>§73.67(d)(3) & (7)</p> | <p>Monitor, with an intrusion alarm or other device or procedures, the controlled access areas, to detect unauthorized penetrations or activities.</p> <p>§73.67(f)(2)</p> |

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems (cont.)

| Component | Category I | Category II | Category III |
|--|---|--|---|
| 2.7.4 Duress Alarms | <p>All manned access control points in the PA barrier, all security patrols, guard stations, and both alarm stations within the PAs, must be provided with duress alarms.</p> <p>§73.46(e)(4)</p> | <p>Under the provisions in Part 73, duress alarms are not required.</p> | <p>Under the provisions in Part 73, duress alarms are not required.</p> |
| 2.7.5 Central and Secondary Alarm Stations | <p>All alarms required pursuant to §73.46 (e) must annunciate in a continuously manned central alarm station (CAS) within the PA and in at least one other independent continuously manned onsite station not necessarily within the PA, so that a single act cannot remove the capability of calling for assistance or responding to an alarm.</p> | <p>Under the provisions in Part 73 central and secondary alarm stations are not required; however, controlled access areas must be monitored with an intrusion alarm or other devices or procedures.</p> <p>§73.67(d)(3)</p> | <p>Under the provisions in Part 73, central and secondary alarm stations are not required; however, controlled access areas must be monitored with an intrusion alarm or other devices or procedures.</p> <p>§73.67(f)(2)</p> |

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems (cont.)

| Component | Category I | Category II | Category III |
|---|--|-------------|--------------|
| <p>2.7.5 Central and Secondary Alarm Stations (cont.)</p> | <p>Annunciate emergency exit alarms in continuously manned CAS located within the PA and in one other continuously manned onsite alarm station.</p> <p>CAS must be located within a building so that the interior of the CAS is not visible from perimeter of PA.</p> <p>CAS cannot contain any operational activities that would interfere with the execution of alarm response functions.</p> <p>The annunciation of an alarm at the alarm station must indicate the type and location of the alarm. The status of all alarms and alarm zones must be indicated in the alarm stations.</p> <p>§73.46(e)(3),(5)&(7)</p> | | |

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems (cont.)

| Component | Category I | Category II | Category III |
|-----------------------------|---|--|--|
| 2.7.6 Power Sources | <p>All alarms required by §73.46(e) must remain operable, from independent power sources in the event of the loss of normal power.</p> <p>Switchover to standby power sources must be automatic and should not cause false alarms on annunciator modules.</p> <p>§73.46(e)(6)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for independent power sources for alarms.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for independent power sources for alarms.</p> |
| 2.7.7 Component Supervision | <p>All alarm devices, including transmission lines to annunciators, must be tamper-indicating and self-checking (e.g., an automatic indication must be provided when a failure of the alarm system or a component occurs, when there is an attempt to compromise the system, or when the system is on standby power).</p> <p>§73.46(e)(7)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for tamper indicating and self checking devices for alarms.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for tamper indicating and self checking devices for alarms.</p> |

¹See general guidance in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," Rev. 3.

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems (cont.)

| Component | Category I | Category II | Category III |
|--|--|---|---|
| 2.7.8 External PA Monitoring & Assessment | <p>All exterior areas within the PA must be monitored or periodically checked to detect the presence of unauthorized persons, activities, vehicles, or materials.</p> <p>§73.46(e)(8)</p> | <p>Under the provisions in Part 73, PAs are not required. However, the controlled access areas must be monitored to detect unauthorized penetrations or activities.</p> <p>§73.67(d)(3)</p> | <p>Under the provisions in Part 73, PAs are not required. However, the controlled access areas must be monitored to detect unauthorized penetrations or activities.</p> <p>§73.67(f)(2)</p> |
| 2.7.9 Observation Methods within MAA and Controlled Access Areas | <p>Methods to observe individuals, within MAA, to assure that SSNM is not moved to unauthorized locations, or in an unauthorized manner, must be provided and used continuously.</p> <p>§73.46(e)(9)</p> | <p>Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetration or activities.</p> <p>§73.67(d)(3)</p> | <p>Monitor with an intrusion alarm, or other device or procedures, the controlled access areas.</p> <p>§73.67(f)(2)</p> |

2.7 Module VII: Detection, Surveillance, and Alarm Subsystems (cont.)

| Component | Category I | Category II | Category III |
|----------------|--|--|--|
| 2.7.10 Records | <p>The licensee must maintain a record, at each onsite alarm annunciation location, of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, alarm circuit, date, and time. In addition, details of response by facility guards or watchman to each alarm, intrusion, or other security incident must be recorded. These records must be retained for 3 years.</p> <p>§73.70(f)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for records of alarms to be retained.</p> | <p>Under the provisions in Part 73, there are no explicit requirements for records of alarms to be retained.</p> |

2.8 Module VIII: Communications Subsystems

| Component | Category I | Category II | Category III |
|--|---|--|--|
| 2.8.1 Security Force Communications | <p>Each guard, watchman, or armed response individual on duty must be capable of maintaining continuous communication, with an individual in each continuously manned alarm station, who will be capable of calling for assistance from other security force personnel and law enforcement authorities.</p> <p>§73.46(f)(1)</p> | <p>Provide a communication capability between the security organization and appropriate response force.</p> <p>§73.67(d)(9)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for security force communications. However, response procedures must be established assuring that a watchman or offsite response force will respond to all unauthorized penetrations or activities.</p> <p>§73.67(f)(3)&(4)</p> |
| 2.8.2 Alarm Station Communications | <p>Each alarm station must be provided with both conventional telephone service and radio or microwave-transmitted two-way voice communication, either directly or through an intermediary, for the capability of communicating with the law enforcement authorities.</p> <p>§73.46(f)(2)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for alarm stations.</p> | <p>Under the provisions in Part 73, there are no explicit requirements for alarm stations.</p> |
| 2.8.3 Independent Power Sources for Communications Equipment | <p>Non-portable communications equipment controlled by the licensee must remain operable from independent power sources for use in the event of loss of normal power.</p> <p>§73.46(f)(3)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for independent power sources for communications equipment.</p> | <p>Under the provisions in Part 73, there are no explicit requirements for independent power sources for communications equipment.</p> |

2.9 Module IX: Test and Maintenance Program for Physical Protection Equipment

| Component | Category I | Category II | Category III |
|------------------------------------|---|---|---|
| 2.9.1 Test and Maintenance Program | <p>A test and maintenance program for intrusion alarms, emergency exit alarms, communications equipment, physical barriers, and other physical protection-related devices and equipment used, pursuant to Part 73, must be established. The program must provide for test and inspections, during installation and construction of physical protection-related subsystems and components, to assure that these devices and equipment comply with their respective design criteria and performance specifications.</p> <p>§73.46(g)(1)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for a test and maintenance program of physical protection-related subsystems and components.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for a test and maintenance program of physical protection-related subsystems and components.</p> |
| 2.9.2 Pre-Operational Tests | <p>The test and maintenance program must provide for preoperational tests and inspections of physical protection-related subsystems and components, to demonstrate their effectiveness and availability with respect to their respective design criteria and performance specifications.</p> <p>§73.46(g)(2)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for pre-operational testing of physical protection-related subsystems and components.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for pre-operational testing of physical protection-related subsystems and components.</p> |

¹See general guidance in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," Rev. 3.

2.9 Module IX: Test and Maintenance Program for Physical Protection Equipment (cont.)

| Component | Category I | Category II | Category III |
|-------------------------|---|---|---|
| 2.9.3 Operational Tests | <p>The test and maintenance program must provide for operational tests and inspections of physical protection- related subsystems and components, to assure their maintenance in an operable and effective condition.</p> <p>Each intrusion alarm must be tested at the beginning and end of any period where it is used. If the period of continuous use is longer than 7 days, the intrusion alarm must be tested at least once every 7 days.</p> <p>Communications equipment required for communications onsite, including duress alarms, for performance must be tested not less than once at the beginning of each security personnel work shift.</p> <p>Communications equipment required for communications offsite must be tested for performance not less than once a day.</p> <p>§73.46(g)(3)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for operational testing of physical protection- related subsystems and components.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for operational testing of physical protection- related subsystems and components.</p> |

¹See general guidance in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," Rev. 3.

2.9 Module IX: Test and Maintenance Program for Physical Protection Equipment (cont.)

| Component | Category I | Category II | Category III |
|--|---|---|---|
| <p>2.9.4 Preventive Maintenance Programs</p> | <p>Preventative maintenance programs for physical protection-related subsystems and components must be established, to assure such subsystems and components continued maintenance in an operable and effective condition.</p> <p>All physical protection-related subsystems and components must be maintained in operable condition.</p> <p>Corrective action procedures and compensatory measures must be developed and employed to assure that the effectiveness of the physical protection system is not reduced by failure or other contingencies affecting the operation of the security-related equipment or structures.</p> <p>§73.46(g)(4)&(5)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for preventative maintenance programs for physical protection-related subsystems and components.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for preventative maintenance programs for physical protection-related subsystems and components.</p> |

¹See general guidance in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," Rev. 3.

2.9 Module IX: Test and Maintenance Program for Physical Protection Equipment (cont.)

| Component | Category I | Category II | Category III |
|-------------------------------|--|---|---|
| 2.9.5 Repairs and Maintenance | <p>Repairs and maintenance must be performed by at least two individuals, working as a team, who have been trained in the operation and performance of the equipment. The security organization must be notified before and after service is performed and must conduct performance verification tests after the service has been completed.</p> <p>§73.46(g)(5)</p> | <p>Under the provisions in Part 73, there are no explicit requirements for repair and maintenance of the physical protection-related subsystems and components.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements for repair and maintenance of the physical protection-related subsystems and components.</p> |
| 2.9.6 Reviews and Audits | <p>Security programs must be reviewed at least every 12 months by individuals, independent of both security program management and personnel, who have direct responsibility for implementation of the security program.</p> <p>The security program review must include an audit of security procedures and practices, an evaluation of the effectiveness of the physical protection system, an audit of the physical protection system testing and maintenance program, and an audit of commitments established for response by Local Law Enforcement Agencies (LLEA).</p> <p>§73.46(g)(6)</p> | <p>Under the provisions in 10 CFR Part 73, there are no explicit requirements for reviews and audits.¹</p> | <p>Under the provisions in 10 CFR Part 73, there are no explicit requirements for reviews and audits.</p> |

¹See general guidance in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," Rev. 3.

2.9 Module IX: Test and Maintenance Program for Physical Protection Equipment (cont.)

| Component | Category I | Category II | Category III |
|---------------|--|--|--|
| 2.9.7 Records | <p>The results and recommendations of the security program review, and any actions taken, must be documented, in a report to the licensee's plant manager, and to corporate management at least one level higher than that having responsibility for the day-to-day plant operations.</p> <p>The results of the security program review must be retained in an auditable form, available for inspection for a period of 3 years.</p> <p>The licensee must retain documentation of all routine security tours and inspections, and of all tests, inspections, and maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security-related equipment used pursuant to the requirements of this part. This documentation must be retained for 3 years.</p> <p>§73.46(g)(6) and §73.70(e)</p> | <p>Under the provisions in Part 73, there are no explicit requirements to retain tests and maintenance records on physical protection-related subsystems and components.¹</p> | <p>Under the provisions in Part 73, there are no explicit requirements to retain tests and maintenance records on physical protection-related subsystems and components.</p> |

¹See general guidance in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems," Rev. 3.

2.10 Module X: Contingency Response Plans and Procedures

| Component | Category I | Category II | Category III |
|--|---|--|---|
| <p>2.10.1 Contingency Plan Documentation</p> | <p>An NRC-approved safeguards contingency plan, for responding to threats, thefts, and radiological sabotage related to the SSNM and nuclear facilities subject to §73.46, must be established, maintained, and followed.</p> <p>Safeguards contingency plans must be in accordance with the criteria in Appendix C, Part 73, "Licensee Safeguards Contingency Plans." These plans must include, but not be limited to, the response requirements listed in paragraphs (h)(2) through (h)(5) of §73.46.</p> <p>§73.46(h)(1)</p> | <p>Establish and maintain written response procedures for dealing with threats of theft or theft of material.</p> <p>§73.67(d)(11)</p> | <p>Establish and maintain written response procedures for dealing with threats of theft or theft of material.</p> <p>§73.67(f)(4)</p> |

2.10 Module X: Contingency Response Plans and Procedures (cont.)

| Component | Category I | Category II | Category III |
|----------------------------|---|--|--|
| 2.10.2 LLEA | <p>Response arrangements that have been made with LLEAs must be established and documented.</p> <p>§73.46(h)(2)</p> | <p>Establish and maintain written response procedures for dealing with threats of theft or theft of material.</p> <p>§73.67(d)(11)</p> | <p>Arrangements must be made for a watchman or offsite response force to respond to all unauthorized penetrations or activities. In addition, response procedures for dealing with threats of thefts of material must be established and maintained.</p> <p>§73.67(f)(3)&(4)</p> |
| 2.10.3 Response Procedures | <p>On detection of abnormal presence or activity of persons or vehicles within an isolation zone, a PA, MAA, or a vital area or on evidence or indication of intrusion into a PA, an MAA, or a vital area the licensee security organization must:</p> <p>(1) determine whether a threat exists; (2) assess the extent of the</p> | <p>Written response procedures must be established and maintained for dealing with threats of thefts, or thefts of the material.</p> <p>§ 73.67(d)(11)</p> | <p>Written response procedures must be established and maintained for dealing with threats of thefts, or thefts of the material.</p> <p>§73.67(f)(4)</p> |

2.10 Module X: Contingency Response Plans and Procedures (cont.)

| Component | Category I | Category II | Category III |
|------------------------------------|--|-------------|--------------|
| 2.10.3 Response Procedures (cont.) | threat, if any; and (3) take immediate concurrent measures to neutralize the threat by: a) requiring responding guards or other armed response personnel to: interpose themselves between vital areas and MAAs and any adversary attempting entry for purposes of radiological sabotage or theft of SSNM; and intercept any person exiting with SNM; and (b) informing LLEA of the threat and requesting assistance. §73.46(h)(4) | | |

2.10 Module X: Contingency Response Plans and Procedures (cont.)

| Component | Category I | Category II | Category III |
|-------------------------|---|--|--|
| 2.10.4 Use of Force | <p>Every guard and all response personnel must be instructed to prevent or impede acts of radiological sabotage or theft of SSNM by using force sufficient to counter the force directed at them, including the use of deadly force, when the guard or other armed response person has a reasonable belief that it is necessary in self-defense or in the defense of others.</p> <p>§73.46(h)(5)</p> | <p>Under the provisions in Part 73, there are no requirements for use of force.</p> | <p>Under the provisions in Part 73, there are no requirements for use of force.</p> |
| 2.10.5 Alarm Assessment | <p>The capability of observing isolation zones and the physical barrier at the perimeter of the PA, to facilitate initial response to detection of penetration of the PA and assessment of the existence of a threat, must be provided. This capability should preferably be provided by means of CCTV or by other suitable means that limit exposure of responding personnel to possible attack.</p> | <p>The controlled access areas must be monitored with an intrusion alarm or other device or procedures, to detect unauthorized penetrations or activities.</p> <p>§73.67(d)(3)</p> | <p>The controlled access areas must be monitored with an intrusion alarm or other device or procedures, to detect unauthorized penetrations or activities.</p> <p>73.67(f)(2)§</p> |

2.10 Module X: Contingency Response Plans and Procedures (cont.)

| Component | Category I | Category II | Category III |
|---------------------------------|---|-------------|--------------|
| 2.10.5 Alarm Assessment (cont.) | <p>Alarms occurring within unoccupied vaults and unoccupied MAAs containing unalloyed or unencapsulated SSNM must be assessed by at least two security personnel using CCTV or other remote means.</p> <p>Alarms occurring within unoccupied MAAs that contain only alloyed or encapsulated SSNM must be assessed as in paragraph (h)(7) of §73.46, or by at least two security personnel who must undergo a search before exiting the MAA.</p> <p>§73.46(h)(7)&(8)</p> | | |

2.10 Module X: Contingency Response Plans and Procedures (cont.)

| Component | Category I | Category II | Category III |
|----------------|--|---|---|
| 2.10.6 Records | <p>The current safeguards contingency plan and documentation of the current response arrangements made with the LLEA must be retained as a record until the Commission terminates the license and, if any portion of the plan is superseded, retain the superseded material for 3 years after each change.</p> <p>§73.46(h)(1)&(2)</p> | <p>A copy of the response procedures must be retained as a record for the period during which the licensee possesses the appropriate type and quantity of SNM. These records must be maintained for 3 years thereafter. If any portion of the procedure is superseded, retain the superseded material for 3 years.</p> <p>§73.67(d)(11)</p> | <p>The current response procedures must be retained as a record for 3 years after the close of period for which the licensee possesses the SNM under each license for which the procedures were established. If any portion of the procedure is superseded, retain the superseded material for 3 years.</p> <p>§73.67(f)(4)</p> |

2.11 Module XI: Reporting of Safeguards Events

| Component | Category I | Category II | Category III |
|--|--|--|---|
| 2.11.1 Events to be reported within 1 hour of discovery for facilities possessing SNM. | <p>Any event in which there is reason to believe that a person has committed or caused or attempted to commit or cause or has made a credible threat to commit or cause theft or unlawful diversion of SNM.</p> <p>Appendix G to Part 73</p> | <p>Any event in which there is reason to believe that a person has committed or caused or attempted to commit or cause or has made a credible threat to commit or cause theft or unlawful diversion of SNM.</p> <p>Appendix G to Part 73</p> | <p>Any event in which there is reason to believe that a person has committed or caused or attempted to commit or cause or has made a credible threat to commit or cause theft or unlawful diversion of SNM</p> <p>Appendix G to Part 73</p> |
| 2.11.2 Events to be reported within 1 hour of discovery for facilities possessing SSNM | <p>Any event in which there is reason to believe that a person has committed or caused or attempted to commit or cause or has made a credible threat to commit or cause significant physical damage to any facility possessing SSNM or to the nuclear fuel a facility possesses.</p> | <p>Any event in which there is reason to believe that a person has committed or caused or attempted to commit or cause or has made a credible threat to commit or cause significant physical damage to any facility possessing SSNM or to the nuclear fuel a facility possesses.</p> | <p>Under the provisions in Part 73, there are no explicit requirements for events to be reported within 1 hour of discovery. By definition Category III material does not include SSNM.</p> |

2.11 Module XI: Reporting of Safeguards Events (cont.)

| Component | Category I | Category II | Category III |
|---|--|--|--------------|
| <p>2.11.2 Events to be reported within 1 hour of discovery for facilities possessing SSNM (cont.)</p> | <p>An actual entry of an unauthorized person, into a PA, an MAA, controlled access area, or vital area.</p> <p>Any failure, degradation, or the discovered vulnerability in a safeguards system that could allow unauthorized or undetected access to a PA, an MAA, controlled access area, or vital area for which compensatory measures have not been employed.</p> <p>The actual or attempted introduction of contraband into a PA, an MAA, or vital area.</p> <p>Appendix G to Part 73</p> | <p>An actual entry of an unauthorized person, into a PA, an MAA, controlled access area, or vital area.</p> <p>Any failure, degradation, or the discovered vulnerability in a safeguards system that could allow unauthorized or undetected access to a PA, an MAA, controlled access area, or vital area for which compensatory measures have not been employed.</p> <p>The actual or attempted introduction of contraband into a PA, an MAA, or vital area.</p> <p>Appendix G to Part 73</p> | |

2.11 Module XI: Reporting of Safeguards Events (cont.)

| Component | Category I | Category II | Category III |
|---|--|--|--|
| <p>2.11.3 Events required to be logged within 24 hours of discovery</p> | <p>Any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to a PA, an MAA, controlled access area, or vital area had compensatory measures not been established.</p> <p>Any other threatened, attempted, or committed act not previously defined in Appendix G to Part 73 with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of reduction of effectiveness.</p> <p>Appendix G to Part 73</p> | <p>Any failure, degradation, or discovered vulnerability in a safeguards system that could have allowed unauthorized or undetected access to a PA, an MAA, controlled access area, or vital area had compensatory measures not been established.</p> <p>Any other threatened, attempted, or committed act not previously defined in Appendix G to Part 73 with the potential for reducing the effectiveness of the safeguards system below that committed to in a licensed physical security or contingency plan or the actual condition of reduction of effectiveness.</p> <p>Appendix G to Part 73</p> | <p>Under the provisions in Part 73, there are no explicit requirements for events to be logged within 24 hours of discovery.</p> |

2.11 Module XI: Reporting of Safeguards Events (cont.)

| Component | Category I | Category II | Category III |
|---|--|--|--|
| <p>2.11.4 Notification to NRC of 1 hour reportable events</p> | <p>Notification must be made to the NRC Operations Center via the Emergency Notification System, if the licensee is party to that system.</p> <p>If the Emergency Notification System is inoperative or unavailable, the licensee must make the required notification via commercial telephone service or other dedicated telephone system or any other methods that will ensure that a report is received by the NRC Operating Center within 1 hour. The exemption of 10 CFR 73.21(g)(3) applies to all telephone reports required by §73.71.</p> <p>The licensee must, on the request of NRC, maintain an open and continuous communication channel with the NRC Operations Center.</p> <p align="center">§73.71(a)(2)&(3)</p> | <p>Notification must be made to the NRC Operations Center via the Emergency Notification System, if the licensee is party to that system.</p> <p>If the Emergency Notification System is inoperative or unavailable, the licensee must make the required notification via commercial telephone service or other dedicated telephone system or any other methods that will ensure that a report is received by the NRC Operating Center within 1 hour. The exemption of 10 CFR 73.21(g)(3) applies to all telephone reports required by §73.71.</p> <p>The licensee must, on the request of NRC, maintain an open and continuous communication channel with the NRC Operations Center.</p> <p align="center">§73.71(a)(2)&(3)</p> | <p>Notification must be made to the NRC Operations Center via the Emergency Notification System, if the licensee is party to that system.</p> <p>If the Emergency Notification System is inoperative or unavailable, the licensee must make the required notification via commercial telephone service or other dedicated telephone system or any other methods that will ensure that a report is received by the NRC Operating Center within 1 hour. The exemption of 10 CFR 73.21(g)(3) applies to all telephone reports required by §73.71.</p> <p>The licensee must, on the request of NRC, maintain an open and continuous communication channel with the NRC Operations Center.</p> <p align="center">§73.71(a)(2)&(3)</p> |

2.11 Module XI: Reporting of Safeguards Events (cont.)

| Component | Category I | Category II | Category III |
|-------------------------|--|--|--|
| 2.11.5 Report submittal | <p>The initial telephone notification must be followed within a period of 30 days by a written report submitted to NRC, Document Control Desk, Washington, DC 20555.</p> <p>A copy of the report must also be submitted to the appropriate NRC Regional Office listed in Appendix A to Part 73. The report must include sufficient information for NRC analysis and evaluation.</p> <p>Significant supplemental information that becomes available after the initial telephonic notification to the NRC Operations Center, or after the submission of the written report, must be telephonically reported to the NRC Operations Center and also submitted in a revised written report (with the revisions indicated) to the Regional Office and the Document Control Desk. Errors discovered in a written report must be corrected in a revised report, with the revisions indicated. The revised report must replace the previous report; the update must be a complete entity and not contain only supplementary or revised information.</p> | <p>The initial telephone notification must be followed within a period of 30 days by a written report submitted to NRC, Document Control Desk, Washington, DC 20555.</p> <p>A copy of the report must also be submitted to the appropriate NRC Regional Office listed in Appendix A to Part 73. The report must include sufficient information for NRC analysis and evaluation.</p> <p>Significant supplemental information that becomes available after the initial telephonic notification to the NRC Operations Center, or after the submission of the written report, must be telephonically reported to the NRC Operations Center and also submitted in a revised written report (with the revisions indicated) to the Regional Office and the Document Control Desk. Errors discovered in a written report must be corrected in a revised report, with the revisions indicated. The revised report must replace the previous report; the update must be a complete entity and not contain only supplementary or revised information.</p> | <p>The initial telephone notification must be followed within a period of 30 days by a written report submitted to NRC, Document Control Desk, Washington, DC 20555.</p> <p>A copy of the report must also be submitted to the appropriate NRC Regional Office listed in Appendix A to Part 73. The report must include sufficient information for NRC analysis and evaluation.</p> <p>Significant supplemental information that becomes available after the initial telephonic notification to the NRC Operations Center, or after the submission of the written report, must be telephonically reported to the NRC Operations Center and also submitted in a revised written report (with the revisions indicated) to the Regional Office and the Document Control Desk. Errors discovered in a written report must be</p> |

2.11 Module XI: Reporting of Safeguards Events (cont.)

| Component | Category I | Category II | Category III |
|--|--|--|---|
| <p>2.11.5 Report submittal (continued)</p> | <p>The 30-day written report required under the provisions of §73.71 must be submitted and of a quality that will permit legible reproductions and processing.</p> <p>The licensee must prepare the written report in letter format and must include sufficient information for NRC analysis and evaluation.</p> <p>§73.71(a)(4)&(5) and (d)</p> | <p>The 30-day written report required under the provisions of §73.71 must be submitted and of a quality that will permit legible reproductions and processing.</p> <p>The licensee must prepare the written report in letter format and must include sufficient information for NRC analysis and evaluation.</p> <p>§73.71(a)(4)&(5) and (d)</p> | <p>corrected in a revised report, with the revisions indicated. The revised report must replace the previous report, the update must be a complete entity and not contain only supplementary or revised information.</p> <p>The 30-day written report required under the provisions of §73.71 must be submitted and of a quality that will permit legible reproductions and processing.</p> <p>The licensee must prepare the written report in letter format and must include sufficient information for NRC analysis and evaluation.</p> <p>§73.71(a)(4)&(5) and (d)</p> |

2.11 Module XI: Reporting of Safeguards Events (cont.)

| Component | Category I | Category II | Category III |
|-----------------------------|---|---|---|
| 2.11.6 Safeguards Event Log | <p>Licensees must maintain a current log and record the safeguards events described in paragraphs II(a) and (b) of Appendix G to Part 73 within 24 hours of discovery by a licensee employee or member of the licensee's contract security organization.</p> <p>§73.71(c)</p> | <p>Licensees must maintain a current log and record the safeguards events described in paragraphs II(a) and (b) of Appendix G to Part 73 within 24 hours of discovery by a licensee employee or member of the licensee's contract security organization.</p> <p>§73.71(c)</p> | <p>Under the provisions in Part 73, there are no explicit requirements to maintain a safeguards event log.</p> |
| 2.11.7 Records | <p>Copies of the written report of an event must be maintained as a record for 3 years from the date of the report.</p> <p>The log of events must be retained for three years after the last entry is made.</p> <p>§73.71(a)(5)&(c)</p> | <p>Copies of the written report of an event must be maintained as a record for 3 years from the date of the report.</p> <p>The log of events must be retained for three years after the last entry is made.</p> <p>§73.71(a)(5)&(c)</p> | <p>Under the provisions in Part 73, there are no explicit requirements to maintain copies of written reports.</p> |

APPENDIX B – GLOSSARY OF TERMS

These terms are excerpted from Title 10 of the *Code of Federal Regulations* (10 CFR Part 73).

Armed response personnel - Persons not necessarily uniformed, whose primary duty in the event of attempted theft of special nuclear material or radiological sabotage is to respond, armed and equipped, to prevent or delay such actions.

Authorized individual - Any individual, including an employee, a student, a consultant, or an agent of a licensee who has been designated in writing by a licensee to have responsibility for surveillance of or control over special nuclear material or to have unescorted access to areas where special nuclear material is used or stored.

Category I - A formula quantity of strategic special nuclear material (SSNM) SSNM in any combination in a quantity of 5,000 grams or more computed by the formula, grams=(grams contained U-235) + 2.5(grams U-233 + grams plutonium).]

Category II - Special nuclear material (SNM) of moderate strategic significance [(1) less than a formula quantity of SSNM but more than 1,000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope) or more than 500 grams of U-233 or plutonium or in a combined quantity of more than 1,000 grams when computed by the equation, grams = (grams contained U-235) + 2(grams U-233 + grams plutonium); or 2) 10,000 grams or more of U-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U-235 isotope).]

Category III - SNM of low strategic significance.[1) less than an amount of SNM of moderate strategic significance but more than 15 grams of U-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope) or 15 grams of U-233 or 15 grams of plutonium or the combination of 15 grams when computed by the equation, grams = (grams contained U-235) + (grams plutonium) + (grams U-233); or 2) Less than 10,000 grams but more than 1,000 grams of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U-2325 isotope); or 3) 10,000 grams or more of uranium-235 (contained in uranium enriched above natural but less than 10 percent in the U-235 isotope).]

Controlled access area - Any temporarily or permanently established area which is clearly demarcated, access to which is controlled and which affords isolation of the material or persons within it.

Deceit - Methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear materials, where the attempt involves falsification to present the appearance of authorized access.

Force - Violent methods used by an adversary to attempt to steal strategic special nuclear material or to sabotage a nuclear facility or violent methods used by response personnel to protect against such adversary actions.

Guard - A uniformed individual armed with a firearm whose primary duty is the protection of special nuclear material against theft, the protection of a plant against radiological sabotage, or both.

Incendiary device - Any self contained device intended to create an intense fire that can damage normally flame-resistant or retardant materials.

Intrusion alarm - A tamper indicating electrical, electromechanical, electrooptical, electronic or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals.

Isolation zone - Any area adjacent to a physical barrier, clear of all objects that could conceal or shield an individual.

Material access area - any location which contains special nuclear material, within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier.

Physical barrier – (1) Fences constructed of No.11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire (or similar material) on brackets angled inward or outward between 30 degrees and 45 degrees from the vertical, with an overall height of not less than 2.4 meters [8 feet], including the barbed topping; (2) building walls, ceilings, and floors constructed of stone, brick, cinder block, concrete, steel, or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength so that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping (as described in item 1 of this definition) of a height of not less than 2.4 meters [8 feet]; or (3) any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.

Protected area - An area encompassed by physical barriers and to which access is controlled.

Stealth - Methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear material, where the fact of such attempt is concealed or an attempt is made to conceal it.

Strategic special nuclear material – Uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium.

Tactical Response Team - The primary response force for each shift which can be identified by a distinctive item of uniform, armed with specified weapons, and whose other duties permit immediate response.

Vault - A windowless enclosure with walls, floor, roof and door(s) designed and constructed to delay penetration from forced entry.

Vault-type room - A room with one or more doors, all capable of being locked, protected by an intrusion alarm which creates an alarm upon the entry of a person anywhere into the room and upon exit from the room or upon movement of an individual within the room.

Watchman – An individual, not necessarily uniformed or armed with a firearm, who provides protection for a plant and the special nuclear material therein in the course of performing other duties.