AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(iii) Adversely impact the operation of systems, networks, and associated equipment.

(b) To accomplish this, the licensee shall:

(1) Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,

(2) Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section; and

(3) Incorporate the cyber security program as a component of the physical protection program.

(c) The cyber security program must be designed to:

(1) Implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks;

(2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks;

(3) Mitigate the adverse affects of cyber attacks; and

(4) Ensure that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks.

(d) As part of the cyber security program, the licensee shall:

(1) Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.

(2) Evaluate and manage cyber risks.

(3) Ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained.

(e) The licensee shall establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of this section.

(1) The cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.

(2) The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will:

(i) Maintain the capability for timely detection and response to cyber attacks;

(ii) Mitigate the consequences of cyber attacks;

(iii) Correct exploited vulnerabilities; and

(iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

(f) The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

(g) The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.

(h) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.

[74 FR 13970, Mar. 27, 2009]

§ 73.55 Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

(a) *Introduction.* (1) By March 31, 2010, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan referred to collectively hereafter as "security plans." Current applicants for

an operating license under 10 CFR part 50, or combined license under 10 CFR part 52 who have submitted their applications to the Commission prior to the effective date of this rule must amend their applications to include security plans consistent with this section.

(2) The security plans must identify, describe, and account for site-specific conditions that affect the licensee's capability to satisfy the requirements of this section.

(3) The licensee is responsible for maintaining the onsite physical protection program in accordance with Commission regulations through the implementation of security plans and written security implementing procedures.

(4) Applicants for an operating license under the provisions of part 50 of this chapter or holders of a combined license under the provisions of part 52 of this chapter, shall implement the requirements of this section before fuel is allowed onsite (protected area).

(5) The Tennessee Valley Authority Watts Bar Nuclear Plant, Unit 2, holding a current construction permit under the provisions of part 50 of this chapter, shall meet the revised requirements in paragraphs (a) through (r) of this section as applicable to operating nuclear power reactor facilities.

(6) Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter that do not reference a standard design certification or reference a standard design certification issued after May 26, 2009 shall meet the requirement of § 73.55(i)(4)(iii).

(b) *General performance objective and requirements.* (1) The licensee shall establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

(2) To satisfy the general performance objective of paragraph (b)(1) of this section, the physical protection program must protect against the design basis threat of radiological sabotage as stated in § 73.1.

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

(i) Ensure that the capabilities to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in § 73.1, are maintained at all times.

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

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

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

(6) The licensee shall establish, maintain, and implement a performance evaluation program in accordance with appendix B to this part, to demonstrate and assess the effectiveness of armed responders and armed security officers to implement the licensee's protective strategy.

(7) The licensee shall establish, maintain, and implement an access authorization program in accordance with § 73.56 and shall describe the program in the Physical Security Plan.

(8) The licensee shall establish, maintain, and implement a cyber security program in accordance with § 73.54.

(9) The licensee shall establish, maintain, and implement an insider mitigation program and shall describe the program in the Physical Security Plan.

(i) The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining

unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage and spent fuel sabotage.

(ii) The insider mitigation program must contain elements from:

(A) The access authorization program described in § 73.56;

(B) The fitness-for-duty program described in part 26 of this chapter;

(C) The cyber security program described in § 73.54; and

(D) The physical protection program described in this section.

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

(11) Implementation of security plans and associated procedures must be coordinated with other onsite plans and procedures to preclude conflict during both normal and emergency conditions.

(c) *Security plans.* (1) Licensee security plans must describe:

(i) How the licensee will implement requirements of this section through the establishment and maintenance of a security organization, the use of security equipment and technology, the training and qualification of security personnel, the implementation of predetermined response plans and strategies, and the protection of digital computer and communication systems and networks.

(ii) Site-specific conditions that affect how the licensee implements Commission requirements.

(2) *Protection of security plans.* The licensee shall protect the security plans and other security-related information against unauthorized disclosure in accordance with the requirements of § 73.21.

(3) *Physical Security Plan.* The licensee shall establish, maintain, and implement a Physical Security Plan which describes how the performance objective and requirements set forth in this section will be implemented.

(4) *Training and Qualification Plan.* The licensee shall establish, maintain, and implement, and follow a Training and Qualification Plan that describes how the criteria set forth in appendix B, to this part, "General Criteria for Security Personnel," will be implemented.

(5) *Safeguards Contingency Plan.* The licensee shall establish, maintain, and implement a Safeguards Contingency Plan that describes how the criteria set forth in appendix C, to this part, "Licensee Safeguards Contingency Plans," will be implemented.

(6) *Cyber Security Plan.* The licensee shall establish, maintain, and implement a Cyber Security Plan that describes how the criteria set forth in § 73.54 "Protection of Digital Computer and Communication systems and Networks" of this part will be implemented.

(7) *Security implementing procedures.* (i) The licensee shall have a management system to provide for the development, implementation, revision, and oversight of security procedures that implement Commission requirements and the security plans.

(ii) Implementing procedures must document the structure of the security organization and detail the types of duties, responsibilities, actions, and decisions to be performed or made by each position of the security organization.

(iii) The licensee shall:

(A) Provide a process for the written approval of implementing procedures and revisions by the individual with overall responsibility for the security program.

(B) Ensure that revisions to security implementing procedures satisfy the requirements of this section.

(iv) Implementing procedures need not be submitted to the Commission for approval, but are subject to inspection by the Commission.

(d) *Security organization.* (1) The licensee shall establish and maintain a security organization that is designed, staffed, trained, qualified, and equipped to implement the physical protection program in accordance with the requirements of this section.

(2) The security organization must include:

(i) A management system that provides oversight of the onsite physical protection program.

(ii) At least one member, onsite and available at all times, who has the authority to direct the activities of the security organization and who is assigned no other duties that would interfere with this individual's ability to perform these duties in accordance with the security plans and the licensee protective strategy.

(3) The licensee may not permit any individual to implement any part of the physical protection program unless the individual has been trained, equipped, and qualified to perform their assigned duties and responsibilities in accordance with appendix B to this part and the Training and Qualification Plan. Non-security personnel may be assigned duties and responsibilities required to implement the physical protection program and shall:

(i) Be trained through established licensee training programs to ensure each individual is trained, qualified, and periodically re-qualified to perform assigned duties.

(ii) Be properly equipped to perform assigned duties.

(iii) Possess the knowledge, skills, and abilities, to include physical attributes such as sight and hearing, required to perform their assigned duties and responsibilities.

(e) *Physical barriers.* Each licensee shall identify and analyze site-specific conditions to determine the specific use, type, function, and placement of physical barriers needed to satisfy the physical protection program design requirements of § 73.55(b).

(1) The licensee shall:

(i) Design, construct, install and maintain physical barriers as necessary to control access into facility areas for which access must be controlled or denied to satisfy the physical protection program design requirements of paragraph (b) of this section.

(ii) Describe in the security plan, physical barriers, barrier systems, and their functions within the physical protection program.

(2) The licensee shall retain, in accordance with § 73.70, all analyses and descriptions of the physical barriers and barrier systems used to satisfy the requirements of this section, and shall protect these records in accordance with the requirements of § 73.21.

(3) Physical barriers must:

(i) Be designed and constructed to:

(A) Protect against the design basis threat of radiological sabotage;

(B) Account for site-specific conditions; and

(C) Perform their required function in support of the licensee physical protection program.

(ii) Provide deterrence, delay, or support access control.

(iii) Support effective implementation of the licensee's protective strategy.

(4) Consistent with the stated function to be performed, openings in any barrier or barrier system established to meet the requirements of this section must be secured and monitored to prevent exploitation of the opening.

(5) *Bullet resisting physical barriers.* The reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed, must be bullet-resisting.

(6) *Owner controlled area.* The licensee shall establish and maintain physical barriers in the owner controlled area as needed to satisfy the physical protection program design requirements of § 73.55(b).

(7) *Isolation zone.* (i) An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be:

(A) Designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier;

(B) Monitored with intrusion detection equipment designed to satisfy the requirements of § 73.55(i) and be capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier; and

(C) Monitored with assessment equipment designed to satisfy the requirements of § 73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation.

(ii) Obstructions that could prevent the licensee's capability to meet the

observation and assessment requirements of this section must be located outside of the isolation zone.

(8) *Protected area.* (i) The protected area perimeter must be protected by physical barriers that are designed and constructed to:

(A) Limit access into the protected area to only those personnel, vehicles, and materials required to perform official duties;

(B) Channel personnel, vehicles, and materials to designated access control portals; and

(C) Be separated from any other barrier designated as a vital area physical barrier, unless otherwise identified in the Physical Security Plan.

(ii) Penetrations through the protected area barrier must be secured and monitored in a manner that prevents or delays, and detects the exploitation of any penetration.

(iii) All emergency exits in the protected area must be alarmed and secured by locking devices that allow prompt egress during an emergency and satisfy the requirements of this section for access control into the protected area.

(iv) Where building walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary provided that the detection and, assessment requirements of this section are met, appropriate barriers are installed, and the area is described in the security plans.

(v) All exterior areas within the protected area, except for areas that must be excluded for safety reasons, must be periodically checked to detect and deter unauthorized personnel, vehicles, and materials.

(9) *Vital areas.* (i) Vital equipment must be located only within vital areas, which must be located within a protected area so that access to vital equipment requires passage through at least two physical barriers, except as otherwise approved by the Commission and identified in the security plans.

(ii) The licensee shall protect all vital area access portals and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements of this section.

(iii) Unoccupied vital areas must be locked and alarmed.

(iv) More than one vital area may be located within a single protected area.

(v) At a minimum, the following shall be considered vital areas:

(A) The reactor control room;

(B) The spent fuel pool;

(C) The central alarm station; and

(D) The secondary alarm station in accordance with § 73.55(i)(4)(iii).

(vi) At a minimum, the following shall be located within a vital area:

(A) The secondary power supply systems for alarm annunciation equipment; and

(B) The secondary power supply systems for non-portable communications equipment.

(10) *Vehicle control measures.* Consistent with the physical protection program design requirements of § 73.55(b), and in accordance with the site-specific analysis, the licensee shall establish and maintain vehicle control measures, as necessary, to protect against the design basis threat of radiological sabotage vehicle bomb assault.

(i) *Land vehicles.* Licensees shall:

(A) Design, construct, install, and maintain a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems necessary to prevent significant core damage and spent fuel sabotage against the effects of the design basis threat of radiological sabotage land vehicle bomb assault.

(B) Periodically check the operation of active vehicle barriers and provide a secondary power source, or a means of mechanical or manual operation in the event of a power failure, to ensure that the active barrier can be placed in the denial position to prevent unauthorized vehicle access beyond the required standoff distance.

(C) Provide periodic surveillance and observation of vehicle barriers and barrier systems adequate to detect indications of tampering and degradation or to otherwise ensure that each vehicle barrier and barrier system is able to satisfy the intended function.

(D) Where a site has rail access to the protected area, install a train derailer, remove a section of track, or restrict access to railroad sidings and provide

periodic surveillance of these measures.

(ii) *Waterborne vehicles.* Licensees shall:

(A) Identify areas from which a waterborne vehicle must be restricted, and where possible, in coordination with local, State, and Federal agencies having jurisdiction over waterway approaches, deploy buoys, markers, or other equipment.

(B) In accordance with the site-specific analysis, provide periodic surveillance and observation of waterway approaches and adjacent areas.

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

(2) The licensee shall consider cyber attacks in the development and identification of target sets.

(3) Target set equipment or elements that are not contained within a protected or vital area must be identified and documented consistent with the requirements in §73.55(f)(1) and be accounted for in the licensee's protective strategy.

(4) The licensee shall implement a process for the oversight of target set equipment and systems to ensure that changes to the configuration of the identified equipment and systems are considered in the licensee's protective strategy. Where appropriate, changes must be made to documented target sets.

(g) *Access controls.* (1) Consistent with the function of each barrier or barrier system, the licensee shall control personnel, vehicle, and material access, as applicable, at each access control point in accordance with the physical protection program design requirements of §73.55(b).

(i) To accomplish this, the licensee shall:

(A) Locate access control portals outside of, or concurrent with, the physical barrier system through which it controls access.

(B) Equip access control portals with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function.

(C) Provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment located at or outside of the protected area.

(D) Limit unescorted access to the protected area and vital areas, during non-emergency conditions, to only those individuals who require unescorted access to perform assigned duties and responsibilities.

(E) Assign an individual the responsibility for the last access control function (controlling admission to the protected area) and isolate the individual within a bullet-resisting structure to assure the ability of the individual to respond or summon assistance.

(ii) Where vehicle barriers are established, the licensee shall:

(A) Physically control vehicle barrier portals to ensure only authorized vehicles are granted access through the barrier.

(B) Search vehicles and materials for contraband or other items which could be used to commit radiological sabotage in accordance with paragraph (h) of this section.

(C) Observe search functions to ensure a response can be initiated if needed.

(2) Before granting access into the protected area, the licensee shall:

(i) Confirm the identity of individuals.

(ii) Verify the authorization for access of individuals, vehicles, and materials.

(iii) Confirm, in accordance with industry shared lists and databases that individuals are not currently denied access to another licensed facility.

(iv) Search individuals, vehicles, and materials in accordance with paragraph (h) of this section.

(3) *Vehicles in the protected area.* (i) The licensee shall exercise control over all vehicles inside the protected area to ensure that they are used only by authorized persons and for authorized purposes.

(ii) Vehicles inside the protected area must be operated by an individual authorized unescorted access to the area, or must be escorted by an individual as required by paragraph (g)(8) of this section.

(iii) Vehicle use inside the protected area must be limited to plant functions or emergencies, and keys must be removed or the vehicle otherwise disabled when not in use.

(iv) Vehicles transporting hazardous materials inside the protected area must be escorted by an armed member of the security organization.

(4) *Vital areas.* (i) Licensees shall control access into vital areas consistent with access authorization lists.

(ii) In response to a site-specific credible threat or other credible information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area.

(5) *Emergency conditions.* (i) The licensee shall design the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions.

(ii) To satisfy the design criteria of paragraph (g)(5)(i) of this section during emergency conditions, the licensee shall implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

(6) *Access control devices.* (i) The licensee shall control all keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise. To accomplish this, the licensee shall:

(A) Issue access control devices only to individuals who have unescorted access authorization and require access to perform official duties and responsibilities.

(B) Maintain a record, to include name and affiliation, of all individuals to whom access control devices have been issued, and implement a process to account for access control devices at least annually.

(C) Implement compensatory measures upon discovery or suspicion that any access control device may have been compromised. Compensatory measures must remain in effect until the compromise is corrected.

(D) Retrieve, change, rotate, deactivate, or otherwise disable access control devices that have been or may have been compromised or when a person with access to control devices has been terminated under less than favorable conditions.

(ii) The licensee shall implement a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas.

(A) Identification badges may be removed from the protected area only when measures are in place to confirm the true identity and authorization for unescorted access of the badge holder before allowing unescorted access to the protected area.

(B) Except where operational safety concerns require otherwise, identification badges must be clearly displayed by all individuals while inside the protected area and vital areas.

(C) The licensee shall maintain a record, to include the name and areas to which unescorted access is granted, of all individuals to whom photo identification badges have been issued.

(iii) Access authorization program personnel shall be issued passwords and combinations to perform their assigned duties and may be excepted from the requirement of paragraph (g)(6)(i)(A) of this section provided they meet the background requirements of § 73.56.

(7) *Visitors.* (i) The licensee may permit escorted access to protected and vital areas to individuals who have not been granted unescorted access in accordance with the requirements of § 73.56 and part 26 of this chapter. The licensee shall:

(A) Implement procedures for processing, escorting, and controlling visitors.

(B) Confirm the identity of each visitor through physical presentation of a recognized identification card issued by a local, State, or Federal government agency that includes a photo or contains physical characteristics of the individual requesting escorted access.

(C) Maintain a visitor control register in which all visitors shall register their name, date, time, purpose of visit, employment affiliation, citizenship, and name of the individual to be visited before being escorted into any protected or vital area.

(D) Issue a visitor badge to all visitors that clearly indicates an escort is required.

(E) Escort all visitors, at all times, while inside the protected area and vital areas.

(F) Deny escorted access to any individual who is currently denied access in industry shared data bases.

(ii) Individuals not employed by the licensee but who require frequent or extended unescorted access to the protected area and/or vital areas to perform duties and responsibilities required by the licensee at irregular or intermittent intervals, shall satisfy the access authorization requirements of § 73.56 and part 26 of this chapter, and shall be issued a non-employee photo identification badge that is easily distinguished from other identification badges before being allowed unescorted access to the protected and vital areas. Non-employee photo identification badges must visually reflect that the individual is a non-employee and that no escort is required.

(8) *Escorts.* The licensee shall ensure that all escorts are trained to perform escort duties in accordance with the requirements of this section and site training requirements.

(i) Escorts shall be authorized unescorted access to all areas in which they will perform escort duties.

(ii) Individuals assigned to visitor escort duties shall be provided a means of timely communication with security personnel to summon assistance when needed.

(iii) Individuals assigned to vehicle escort duties shall be trained and qualified in accordance with appendix B of this part and provided a means of continuous communication with security personnel to ensure the ability to summon assistance when needed.

(iv) When visitors are performing work, escorts shall be generally knowledgeable of the activities to be performed by the visitor and report behaviors or activities that may constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage, consistent with § 73.56(f)(1).

(v) Each licensee shall describe visitor to escort ratios for the protected area and vital areas in physical security plans. Implementing procedures shall provide necessary observation and control requirements for all visitor activities.

(h) *Search programs.* (1) The objective of the search program is to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage. To accomplish this the licensee shall search individuals, vehicles, and materials consistent with the physical protection program design requirements in paragraph (b) of this section, and the function to be performed at each access control point or portal before granting access.

(2) *Owner controlled area searches.* (i) Where the licensee has established physical barriers in the owner controlled area, the licensee shall implement search procedures for access control points in the barrier.

(ii) For each vehicle access control point, the licensee shall describe in implementing procedures areas of a vehicle to be searched, and the items for which the search is intended to detect and prevent access. Areas of the vehicle to be searched must include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area.

(iii) Vehicle searches must be performed by at least two (2) trained and equipped security personnel, one of which must be armed. The armed individual shall be positioned to observe the search process and provide immediate response.

(iv) Vehicle searches must be accomplished through the use of equipment capable of detecting firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage, or through visual and physical searches, or both, to ensure that all items are identified before granting access.

(v) Vehicle access control points must be equipped with video surveillance equipment that is monitored by an individual capable of initiating a response.

(3) Protected area searches. Licensees shall search all personnel, vehicles and

materials requesting access to protected areas.

(i) The search for firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage shall be accomplished through the use of equipment capable of detecting these items, or through visual and physical searches, or both, to ensure that all items are clearly identified before granting access to protected areas. The licensee shall subject all persons except official Federal, state, and local law enforcement personnel on official duty to these searches upon entry to the protected area. Armed security officers who are on duty and have exited the protected area may re-enter the protected area without being searched for firearms.

(ii) Whenever search equipment is out of service, is not operating satisfactorily, or cannot be used effectively to search individuals, vehicles, or materials, a visual and physical search shall be conducted.

(iii) When an attempt to introduce firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage has occurred or is suspected, the licensee shall implement actions to ensure that the suspect individuals, vehicles, and materials are denied access and shall perform a visual and physical search to determine the absence or existence of a threat.

(iv) For each vehicle access portal, the licensee shall describe in implementing procedures areas of a vehicle to be searched before access is granted. Areas of the vehicle to be searched must include, but are not limited to, the cab, engine compartment, undercarriage, and cargo area.

(v) Exceptions to the protected area search requirements for materials may be granted for safety or operational reasons provided the design criteria of § 73.55(b) are satisfied, the materials are clearly identified, the types of exceptions to be granted are described in the security plans, and the specific security measures to be implemented for excepted items are detailed in site procedures.

(vi) To the extent practicable, excepted materials must be positively controlled, stored in a locked area, and opened at the final destination by an individual familiar with the items.

(vii) Bulk material excepted from the protected area search requirements must be escorted by an armed member of the security organization to its final destination or to a receiving area where the excepted items are offloaded and verified.

(viii) To the extent practicable, bulk materials excepted from search shall not be offloaded adjacent to a vital area.

(i) *Detection and assessment systems.* (1) The licensee shall establish and maintain intrusion detection and assessment systems that satisfy the design requirements of § 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the licensee's protective strategy.

(2) Intrusion detection equipment must annunciate and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations, at least one of which must be protected in accordance with the requirements of the central alarm station within this section.

(3) The licensee's intrusion detection and assessment systems must be designed to:

(i) Provide visual and audible annunciation of the alarm.

(ii) Provide a visual display from which assessment of the detected activity can be made.

(iii) Ensure that annunciation of an alarm indicates the type and location of the alarm.

(iv) Ensure that alarm devices to include transmission lines to annunciators are tamper indicating and self-checking.

(v) Provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply.

(vi) Support the initiation of a timely response in accordance with the security plans, licensee protective strategy, and associated implementing procedures.

(vii) Ensure intrusion detection and assessment equipment at the protected

area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.

(4) *Alarm stations.* (i) Both alarm stations required by paragraph (i)(2) of this section must be designed and equipped to ensure that a single act, in accordance with the design basis threat of radiological sabotage defined in § 73.1(a)(1), cannot disable both alarm stations. The licensee shall ensure the survivability of at least one alarm station to maintain the ability to perform the following functions:

(A) Detect and assess alarms;

(B) Initiate and coordinate an adequate response to an alarm;

(C) Summon offsite assistance; and

(D) Provide command and control.

(ii) Licensees shall:

(A) Locate the central alarm station inside a protected area. The interior of the central alarm station must not be visible from the perimeter of the protected area.

(B) Continuously staff each alarm station with at least one trained and qualified alarm station operator. The alarm station operator must not be assigned other duties or responsibilities which would interfere with the ability to execute the functions described in § 73.55(i)(4)(i) of this section.

(C) Not permit any activities to be performed within either alarm station that would interfere with an alarm station operator's ability to execute assigned duties and responsibilities.

(D) Assess and initiate response to all alarms in accordance with the security plans and implementing procedures.

(E) Assess and initiate response to other events as appropriate.

(F) Ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the alarm station operator in the other alarm station.

(G) Ensure that operators in both alarm stations are knowledgeable of final disposition of all alarms.

(H) Maintain a record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm.

(iii) Applicants for an operating license under the provisions of part 50 of this chapter, or holders of a combined license under the provisions of part 52 of this chapter, shall construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station contained in this section. Both alarm stations shall be equal and redundant, such that all functions needed to satisfy the requirements of this section can be performed in both alarm stations.

(5) *Surveillance, observation, and monitoring.* (i) The physical protection program must include surveillance, observation, and monitoring as needed to satisfy the design requirements of § 73.55(b), identify indications of tampering, or otherwise implement the site protective strategy.

(ii) The licensee shall provide continuous surveillance, observation, and monitoring of the owner controlled area as described in the security plans to detect and deter intruders and ensure the integrity of physical barriers or other components and functions of the onsite physical protection program. Continuous surveillance, observation, and monitoring responsibilities may be performed by security personnel during continuous patrols, through use of video technology, or by a combination of both.

(iii) Unattended openings that intersect a security boundary such as underground pathways must be protected by a physical barrier and monitored by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation.

(iv) Armed security patrols shall periodically check external areas of the protected area to include physical barriers and vital area portals.

(v) Armed security patrols shall periodically inspect vital areas to include the physical barriers used at all vital area portals.

(vi) The licensee shall provide random patrols of all accessible areas containing target set equipment.

(vii) Security personnel shall be trained to recognize obvious indications of tampering consistent with

their assigned duties and responsibilities.

(viii) Upon detection of tampering, or other threats, the licensee shall initiate response in accordance with the security plans and implementing procedures.

(6) *Illumination.* (i) The licensee shall ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of § 73.55(b) and implement the protective strategy.

(ii) The licensee shall provide a minimum illumination level of 0.2 footcandles, measured horizontally at ground level, in the isolation zones and appropriate exterior areas within the protected area. Alternatively, the licensee may augment the facility illumination system by means of low-light technology to meet the requirements of this section or otherwise implement the protective strategy.

(iii) The licensee shall describe in the security plans how the lighting requirements of this section are met and, if used, the type(s) and application of low-light technology.

(j) *Communication requirements.* (1) The licensee shall establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

(2) Individuals assigned to each alarm station shall be capable of calling for assistance in accordance with the security plans and the licensee's procedures.

(3) All on-duty security force personnel shall be capable of maintaining continuous communication with an individual in each alarm station, and vehicle escorts shall maintain continuous communication with security personnel. All personnel escorts shall maintain timely communication with the security personnel.

(4) The following continuous communication capabilities must terminate in both alarm stations required by this section:

(i) Radio or microwave transmitted two-way voice communication, either directly or through an intermediary, in addition to conventional telephone service between local law enforcement authorities and the site.

(ii) A system for communication with the control room.

(5) Non-portable communications equipment must remain operable from independent power sources in the event of the loss of normal power.

(6) The licensee shall identify site areas where communication could be interrupted or cannot be maintained, and shall establish alternative communication measures or otherwise account for these areas in implementing procedures.

(k) *Response requirements.* (1) The licensee shall establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats up to and including the design basis threat of radiological sabotage as defined in § 73.1, to prevent significant core damage and spent fuel sabotage.

(2) The licensee shall ensure that all firearms, ammunition, and equipment necessary to implement the site security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

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

(4) The licensee shall provide armed response personnel consisting of armed responders which may be augmented with armed security officers to carry out armed response duties within predetermined time lines specified by the site protective strategy.

(5) *Armed responders.* (i) The licensee shall determine the minimum number of armed responders necessary to satisfy the design requirements of § 73.55(b) and implement the protective strategy. The licensee shall document this number in the security plans.

(ii) The number of armed responders shall not be less than ten (10).

(iii) Armed responders shall be available at all times inside the protected area and may not be assigned other duties or responsibilities that could interfere with their assigned response duties.

(6) *Armed security officers.* (i) Armed security officers, designated to strengthen onsite response capabilities, shall be onsite and available at all times to carry out their assigned response duties.

(ii) The minimum number of armed security officers designated to strengthen onsite response capabilities must be documented in the security plans.

(7) The licensee shall have procedures to reconstitute the documented number of available armed response personnel required to implement the protective strategy.

(8) *Protective strategy.* The licensee shall establish, maintain, and implement a written protective strategy in accordance with the requirements of this section and part 73, appendix C, Section II. Upon receipt of an alarm or other indication of a threat, the licensee shall:

(i) Determine the existence and level of a threat in accordance with pre-established assessment methodologies and procedures.

(ii) Initiate response actions to interdict and neutralize the threat in accordance with the requirements of part 73, appendix C, section II, the safeguards contingency plan, and the licensee's response strategy.

(iii) Notify law enforcement agencies (local, State, and Federal law enforcement agencies (LLEA)), in accordance with site procedures.

(9) *Law enforcement liaison.* To the extent practicable, licensees shall document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities.

(10) *Heightened security.* Licensees shall establish, maintain, and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

(i) Licensees shall ensure that the specific protective measures and actions identified for each threat level are consistent with the security plans and other emergency plans and procedures.

(ii) Upon notification by an authorized representative of the Commission, licensees shall implement the specific threat level indicated by the Commission representative.

(l) *Facilities using mixed-oxide (MOX) fuel assemblies containing up to 20 weight percent plutonium dioxide (PuO_2).* (1) Commercial nuclear power reactors licensed under 10 CFR parts 50 or 52 and authorized to use special nuclear material in the form of MOX fuel assemblies containing up to 20 weight percent PuO_2 shall, in addition to meeting the requirements of this section, protect un-irradiated MOX fuel assemblies against theft or diversion as described in this paragraph.

(2) Commercial nuclear power reactors authorized to use MOX fuel assemblies containing up to 20 weight percent PuO_2 are exempt from the requirements of §§ 73.20, 73.45, and 73.46 for the onsite physical protection of un-irradiated MOX fuel assemblies.

(3) *Administrative controls.* (i) The licensee shall describe in the security plans the operational and administrative controls to be implemented for the receipt, inspection, movement, storage, and protection of un-irradiated MOX fuel assemblies.

(ii) The licensee shall implement the use of tamper-indicating devices for un-irradiated MOX fuel assembly transport and shall verify their use and integrity before receipt.

(iii) Upon receipt of un-irradiated MOX fuel assemblies, the licensee shall:

(A) Inspect un-irradiated MOX fuel assemblies for damage.

(B) Search un-irradiated MOX fuel assemblies for unauthorized materials.

(iv) The licensee may conduct the required inspection and search functions simultaneously.

(v) The licensee shall ensure the proper placement and control of un-irradiated MOX fuel assemblies as follows:

(A) At least one armed security officer shall be present during the receipt

and inspection of un-irradiated MOX fuel assemblies. This armed security officer shall not be an armed responder as required by paragraph (k) of this section.

(B) The licensee shall store un-irradiated MOX fuel assemblies only within a spent fuel pool, located within a vital area, so that access to the un-irradiated MOX fuel assemblies requires passage through at least two physical barriers and the water barrier combined with the additional measures detailed in this section.

(vi) The licensee shall implement a material control and accountability program that includes a predetermined and documented storage location for each un-irradiated MOX fuel assembly.

(4) *Physical controls.* (i) The licensee shall lock, lockout, or disable all equipment and power supplies to equipment required for the movement and handling of un-irradiated MOX fuel assemblies when movement activities are not authorized.

(ii) The licensee shall implement a two-person, line-of-sight rule within the spent fuel pool area whenever control systems or equipment required for the movement or handling of un-irradiated MOX fuel assemblies must be accessed.

(iii) The licensee shall conduct random patrols of areas containing un-irradiated MOX fuel assemblies to identify indications of tampering and ensure the integrity of barriers and locks.

(iv) Locks, keys, and any other access control device used to secure equipment and power sources required for the movement of un-irradiated MOX fuel assemblies, or openings to areas containing un-irradiated MOX fuel assemblies, must be controlled by the security organization.

(v) Removal of locks used to secure equipment and power sources required for the movement of un-irradiated MOX fuel assemblies or openings to areas containing un-irradiated MOX fuel assemblies must require approval by both the on-duty security shift supervisor and the operations shift manager.

(A) At least one armed security officer shall be present to observe activities involving the movement of un-irradiated MOX fuel assemblies before the removal of the locks and providing power to equipment required for the movement or handling of un-irradiated MOX fuel assemblies.

(B) At least one armed security officer shall be present at all times until power is removed from equipment and locks are secured.

(C) Security officers shall be knowledgeable of authorized and unauthorized activities involving un-irradiated MOX fuel assemblies.

(5) At least one armed security officer shall be present and shall maintain constant surveillance of un-irradiated MOX fuel assemblies when the assemblies are not located in the spent fuel pool or reactor.

(6) The licensee shall maintain at all times the capability to detect, assess, interdict and neutralize threats to un-irradiated MOX fuel assemblies in accordance with the requirements of this section.

(7) *MOX fuel assemblies containing greater than 20 weight percent* PuO_2. (i) Requests for the use of MOX fuel assemblies containing greater than 20 weight percent PuO_2 shall be reviewed and approved by the Commission before receipt of MOX fuel assemblies.

(ii) Additional measures for the physical protection of un-irradiated MOX fuel assemblies containing greater than 20 weight percent PuO_2 shall be determined by the Commission on a case-by-case basis and documented through license amendment in accordance with 10 CFR 50.90.

(m) *Security program reviews.* (1) As a minimum the licensee shall review each element of the physical protection program at least every 24 months. Reviews shall be conducted:

(i) Within 12 months following initial implementation of the physical protection program or a change to personnel, procedures, equipment, or facilities that potentially could adversely affect security.

(ii) As necessary based upon site-specific analyses, assessments, or other performance indicators.

(iii) By individuals independent of those personnel responsible for program management and any individual who has direct responsibility for implementing the onsite physical protection program.

(2) Reviews of the security program must include, but not be limited to, an audit of the effectiveness of the physical security program, security plans, implementing procedures, cyber security programs, safety/security interface activities, the testing, maintenance, and calibration program, and response commitments by local, State, and Federal law enforcement authorities.

(3) The results and recommendations of the onsite physical protection program reviews, management's findings regarding program effectiveness, and any actions taken as a result of recommendations from prior program reviews, 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 day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection.

(4) Findings from onsite physical protection program reviews must be entered into the site corrective action program.

(n) *Maintenance, testing, and calibration*. (1) The licensee shall:

(i) Establish, maintain, and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

(ii) Describe the maintenance, testing and calibration program in the physical security plan. Implementing procedures must specify operational and technical details required to perform maintenance, testing, and calibration activities to include, but not limited to, purpose of activity, actions to be taken, acceptance criteria, and the intervals or frequency at which the activity will be performed.

(iii) Identify in procedures the criteria for determining when problems, failures, deficiencies, and other findings are documented in the site corrective action program for resolution.

(iv) Ensure that information documented in the site corrective action program is written in a manner that does not constitute safeguards information as defined in 10 CFR 73.21.

(v) Implement compensatory measures that ensure the effectiveness of the onsite physical protection program when there is a failure or degraded operation of security-related component or equipment.

(2) The licensee shall test each intrusion alarm for operability at the beginning and end of any period that it is used for security, or if the period of continuous use exceeds seven (7) days. The intrusion alarm must be tested at least once every seven (7) days.

(3) Intrusion detection and access control equipment must be performance tested in accordance with the security plans and implementing procedures.

(4) Equipment required for communications onsite must be tested for operability not less frequently than once at the beginning of each security personnel work shift.

(5) Communication systems between the alarm stations and each control room, and between the alarm stations and local law enforcement agencies, to include backup communication equipment, must be tested for operability at least once each day.

(6) Search equipment must be tested for operability at least once each day and tested for performance at least once during each seven (7) day period.

(7) A program for testing or verifying the operability of devices or equipment located in hazardous areas must be specified in the implementing procedures and must define alternate measures to be taken to ensure the timely completion of testing or maintenance when the hazardous condition or other restrictions are no longer applicable.

(8) Security equipment or systems shall be tested in accordance with the site maintenance, testing and calibration procedures before being placed back in service after each repair or inoperable state.

(o) *Compensatory measures*. (1) The licensee shall identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components to meet the requirements of this section.

(2) Compensatory measures must provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable, equipment, system, or components.

(3) Compensatory measures must be implemented within specific time frames necessary to meet the requirements stated in paragraph (b) of this section and described in the security plans.

(p) *Suspension of security measures.* (1) The licensee may suspend implementation of affected requirements of this section under the following conditions:

(i) In accordance with §§ 50.54(x) and 50.54(y) of this chapter, the licensee may suspend any security measures under this section in an emergency when this action is immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent. This suspension of security measures must be approved as a minimum by a licensed senior operator before taking this action.

(ii) During severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions and technical specifications can provide adequate or equivalent protection. This suspension of security measures must be approved, as a minimum, by a licensed senior operator, with input from the security supervisor or manager, before taking this action.

(2) Suspended security measures must be reinstated as soon as conditions permit.

(3) The suspension of security measures must be reported and documented in accordance with the provisions of § 73.71.

(q) *Records.* (1) The Commission may inspect, copy, retain, and remove all reports, records, and documents required to be kept by Commission regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

(2) The licensee shall maintain all records required to be kept by Commission regulations, orders, or license conditions, until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.

(3) If a contracted security force is used to implement the onsite physical protection program, the licensee's written agreement with the contractor must be retained by the licensee as a record for the duration of the contract.

(4) Review and audit reports must be maintained and available for inspection, for a period of three (3) years.

(r) *Alternative measures.* (1) The Commission may authorize an applicant or licensee to provide a measure for protection against radiological sabotage other than one required by this section if the applicant or licensee demonstrates that:

(i) The measure meets the same performance objectives and requirements specified in paragraph (b) of this section; and

(ii) The proposed alternative measure provides protection against radiological sabotage or theft of un-irradiated MOX fuel assemblies, equivalent to that which would be provided by the specific requirement for which it would substitute.

(2) The licensee shall submit proposed alternative measure(s) to the Commission for review and approval in accordance with §§ 50.4 and 50.90 of this chapter before implementation.

(3) In addition to fully describing the desired changes, the licensee shall submit a technical basis for each proposed alternative measure. The basis must include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement of this section.

(4) Alternative vehicle barrier systems. In the case of vehicle barrier systems required by § 73.55(e)(10), the licensee shall demonstrate that:

(i) The alternative measure provides protection against the use of a vehicle

as a means of transportation to gain proximity to vital areas;

(ii) The alternative measure provides protection against the use of a vehicle as a vehicle bomb; and

(iii) Based on comparison of the costs of the alternative measures to the costs of meeting the Commission's requirements using the essential elements of 10 CFR 50.109, the costs of fully meeting the Commission's requirements are not justified by the protection that would be provided.

[74 FR 13971, Mar. 27, 2009]

§ 73.56 Personnel access authorization requirements for nuclear power plants.

(a) *Introduction*. (1) By March 31, 2010, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall implement the requirements of this section through revisions to its Commission-approved Physical Security Plan.

(2) The licensee shall establish, implement and maintain its access authorization program in accordance with the requirements of this section.

(3) Each applicant for an operating license under the provisions of part 50 of this chapter, and each holder of a combined license under the provisions of part 52 of this chapter, shall implement the requirements of this section before fuel is allowed on site (protected area).

(4) The licensee or applicant may accept, in part or whole, an access authorization program implemented by a contractor or vendor to satisfy appropriate elements of the licensee's access authorization program in accordance with the requirements of this section. Only a licensee shall grant an individual unescorted access. Licensees and applicants shall certify individuals' unescorted access authorization and are responsible to maintain, deny, terminate, or withdraw unescorted access authorization.

(b) *Applicability*. (1) The following individuals shall be subject to an access authorization program:

(i) Any individual to whom a licensee intends to grant unescorted access to nuclear power plant protected or vital areas or any individual for whom a licensee or an applicant intends to certify unescorted access authorization;

(ii) Any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's or applicant's operational safety, security, or emergency preparedness;

(iii) Any individual who has responsibilities for implementing a licensee's or applicant's protective strategy, including, but not limited to, armed security force officers, alarm station operators, and tactical response team leaders; and

(iv) The licensee or applicant access authorization program reviewing official or contractor or vendor access authorization program reviewers.

(2) Other individuals, at the licensee's or applicant's discretion, including employees of a contractor or a vendor who are designated in access authorization program procedures, are subject to an access authorization program that meets the requirements of this section.

(c) *General performance objective*. The licensee's or applicant's access authorization program must provide high assurance that the individuals who are specified in paragraph (b)(1), and, if applicable, paragraph (b)(2) of this section are trustworthy and reliable, such that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage.

(d) *Background investigation*. In order to grant an individual unescorted access to the protected area or vital area of a nuclear power plant or certify an individual unescorted access authorization, licensees, applicants and contractors or vendors shall ensure that the individual has been subject to a background investigation. The background investigation must include, but is not limited to, the following elements:

(1) *Informed consent*. Licensees, applicants, and contractors or vendors shall not initiate any element of a background investigation without the informed and signed consent of the subject individual. This consent shall include authorization to share personal information with appropriate entities. The licensee or applicant to whom the individual is applying for unescorted