

Code of Federal Regulations]
[Title 10, Volume 2, Parts 51 to 199]
[Revised as of January 1, 2000]
From the U.S. Government Printing Office via GPO Access
[CITE: 10CFR73.55]

TITLE 10--ENERGY

PART 73--PHYSICAL PROTECTION OF PLANTS AND MATERIALS--Table of Contents

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

By Dec. 2, 1986 each licensee, as appropriate, shall submit proposed amendments to its security plan which define how the amended requirements of paragraphs (a), (d)(7), (d)(9), and (e)(1) will be met. Each submittal must include a proposed implementation schedule for Commission approval. The amended safeguards requirements of these paragraphs must be implemented by the licensee within 180 days after Commission approval of the proposed security plan in accordance with the approved schedule.

(a) General performance objective and requirements. The licensee shall establish and maintain an onsite physical protection system and security organization which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in Sec. 73.1(a). To achieve this general performance objective, the onsite physical protection system and security organization must include, but not necessarily be limited to, the capabilities to meet the specific requirements contained in paragraphs (b) through (h) of this section. The Commission may authorize an applicant or licensee to provide measures for protection against radiological sabotage other than those required by this section if the applicant or licensee demonstrates that the measures have the same high assurance objective as specified in this paragraph and that the overall level of system performance provides protection against radiological sabotage equivalent to that which would be provided by paragraphs (b) through (h) of this section and meets the general performance requirements of this section. Specifically, in the special cases of licensed operating reactors with adjacent reactor power plants under construction, the licensee shall provide and maintain a level of physical protection of the operating reactor against radiological sabotage equivalent to the requirements of this section. In accordance with Secs. 50.54(x) and 50.54(y) of part 50, the licensee may suspend any safeguards measures pursuant to Sec. 73.55 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 specification that can provide adequate

or equivalent protection is immediately apparent. This suspension must be approved as a minimum by a licensed senior operator prior to taking the action. The suspension of safeguards measures must be reported in accordance with the provisions of Sec. 73.71. Reports made under Sec. 50.72 need not be duplicated under Sec. 73.71.

(b) Physical Security Organization. (1) The licensee shall establish a security organization, including guards, to protect his facility against radiological sabotage. If a contract guard force is utilized for site security, the licensee's written agreement with the contractor that must be retained by the licensee as a record for the duration of the contract will clearly show that:

(i) The licensee is responsible to the Commission for maintaining safeguards in accordance with Commission regulations and the licensee's security plan,

(ii) The 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 the reports and documents are kept by the licensee or the contractor,

(iii) The requirement in paragraph (b)(4) of this section that the licensee demonstrate the ability of physical security personnel to perform their assigned duties and responsibilities, includes 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

(iv) The contractor will not assign any personnel to the site who have not first been made aware of these responsibilities.

(2) At least one full time member of the security organization who has the authority to direct the physical protection activities of the security organization shall be onsite at all times.

(3) The licensee shall have a management system to provide for the development, revision, implementation, and enforcement of security procedures. The system shall include:

(i) Written security procedures that document the structure of the security organization and detail the duties of guards, watchmen, and other individuals responsible for security. The licensee shall maintain a copy of the current procedures as a record until the Commission terminates each license for which the procedures were developed and, if any portion of the procedure is superseded, retain the superseded material for three years after each change.

(ii) Provision for written approval of these procedures and any revisions to the procedures by the individual with overall responsibility for the security functions. The licensee shall retain each written approval as a record for three years from the date of the approval.

(4)(i) The licensee may not permit an individual to act as a guard, watchman armed response person, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with appendix B, "General Criteria for Security Personnel," to this part. Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities. Each guard, watchman, armed response person, and other member of the security organization shall requalify in accordance with appendix B to

this part at least every 12 months. This requalification must be documented. The licensee shall retain the documentation of each requalification as a record for three years after the requalification.

(ii) Each licensee shall establish, maintain, and follow an NRC-approved training and qualifications plan outlining the processes by which guards, watchmen, armed response persons, and other members of the security organization will be selected, trained, equipped, tested, and qualified to ensure that these individuals meet the requirements of this paragraph. The licensee shall maintain the current training and qualifications plan as a record until the Commission terminates the license for which the plan was developed and, if any portion of the plan is superseded, retain that superseded portion for 3 years after the effective date of the change. The training and qualifications plan must include a schedule to show how all security personnel will be qualified 2 years after the submitted plan is approved. The training and qualifications plan must be followed by the licensee 60 days after the submitted plan is approved by the NRC.

(c) Physical barriers. (1) The licensee shall locate vital equipment only within a vital area, which in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers of sufficient strength to meet the performance requirements of paragraph (a) of this section. More than one vital area may be located within a single protected area.

(2) The physical barriers at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier for a vital area within the protected area.

(3) Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and shall be of sufficient size to permit observation of the activities of people on either side of that barrier in the event of its penetration. If parking facilities are provided for employees or visitors, they shall be located outside the isolation zone and exterior to the protected area barrier.

(4) Detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier shall assure that adequate response by the security organization can be initiated. All exterior areas within the protected area shall be periodically checked to detect the presence of unauthorized persons, vehicles, or materials.

(5) Isolation zones and all exterior areas within the protected area shall be provided with illumination sufficient for the monitoring and observation requirements of paragraphs (c)(3), (c)(4), and (h)(4) of this section, but not less than 0.2 footcandle measured horizontally at ground level.

(6) The walls, doors, ceiling, floor, and any windows in the walls and in the doors of the reactor control room shall be bullet-resisting.

(7) Vehicle control measures, including vehicle barrier systems, must be established to protect against use of a land vehicle, as specified by the Commission, as a means of transportation to gain unauthorized proximity to vital areas.

(8) Each licensee shall compare the vehicle control measures established in accordance with 10 CFR 73.55 (c)(7) to the Commission's design goals (i.e., to protect equipment, systems, devices, or material, the failure of which could directly or indirectly

endanger public health and safety by exposure to radiation) and criteria for protection against a land vehicle bomb. Each licensee shall either:

(i) Confirm to the Commission that the vehicle control measures meet the design goals and criteria specified; or

(ii) Propose alternative measures, in addition to the measures established in accordance with 10 CFR 73.55 (c)(7), describe the level of protection that these measures would provide against a land vehicle bomb, and compare the costs of the alternative measures with the costs of measures necessary to fully meet the design goals and criteria. The Commission will approve the proposed alternative measures if they provide substantial protection against a land vehicle bomb, and it is determined by an analysis, using the essential elements of 10 CFR 50.109, that the costs of fully meeting the design goals and criteria are not justified by the added protection that would be provided.

(9) Each licensee authorized to operate a nuclear power reactor shall:

(i) By February 28, 1995 submit to the Commission a summary description of the proposed vehicle control measures as required by 10 CFR 73.55 (c)(7) and the results of the vehicle bomb comparison as required by 10 CFR 73.55 (c)(8). For licensees who choose to propose alternative measures as provided for in 10 CFR 73.55 (c)(8), the proposal must be submitted in accordance with 10 CFR 50.90 and include the analysis and justification for the proposed alternatives.

(ii) By February 29, 1996 fully implement the required vehicle control measures, including site-specific alternative measures as approved by the Commission.

(iii) Protect as Safeguards Information, information required by the Commission pursuant to 10 CFR 73.55(c) (8) and (9).

(iv) Retain, in accordance with 10 CFR 73.70, all comparisons and analyses prepared pursuant to 10 CFR 73.55 (c) (7) and (8).

(10) Each applicant for a license to operate a nuclear power reactor pursuant to 10 CFR 50.21(b) or 10 CFR 50.22, whose application was submitted prior to August 31, 1994, shall incorporate the required vehicle control program into the site Physical Security Plan and implement it by the date of receipt of the operating license.

(d) Access Requirements. (1) The licensee shall control all points of personnel and vehicle access into a protected area. Identification and search of all individuals unless otherwise provided in this section must be made and authorization must be checked at these points. The search function for detection of firearms, explosives, and incendiary devices must be accomplished through the use of both firearms and explosive detection equipment capable of detecting those devices. The licensee shall subject all persons except bona fide Federal, State, and local law enforcement personnel on official duty to these equipment searches upon entry to a protected area. Armed security guards who are on duty and have exited the protected area may reenter the protected area without being searched for firearms. When the licensee has cause to suspect that an individual is attempting to introduce firearms, explosives, or incendiary devices into protected areas, the licensee shall conduct a physical pat-down search of that individual. Whenever firearms or explosives detection equipment at a portal is out of service or not operating satisfactorily, the licensee shall conduct a physical pat-down search of all

persons who would otherwise have been subject to equipment searches. The individual responsible for the last access control function (controlling admission to the protected area) must be isolated within a bullet-resisting structure as described in paragraph (c)(6) of this section to assure his or her ability to respond or to summon assistance.

(2) At the point of personnel and vehicle access into a protected area, all hand-carried packages shall be searched for devices such as firearms, explosives, and incendiary devices, or other items which could be used for radiological sabotage.

(3) All packages and material for delivery into the protected area shall be checked for proper identification and authorization and searched for devices such as firearms, explosives and incendiary devices or other items which could be used for radiological sabotage, prior to admittance into the protected area, except those Commission approved delivery and inspection activities specifically designated by the licensee to be carried out within vital or protected areas for reasons of safety, security or operational necessity.

(4) All vehicles, except under emergency conditions, must be searched for items which could be used for sabotage purposes prior to entry into the protected area. Vehicle areas to be searched must include the cab, engine compartment, undercarriage, and cargo area. All vehicles, except as indicated in this paragraph, requiring entry into the protected area must be escorted by a member of the security organization while within the protected area and, to the extent practicable, must be off loaded in the protected area at a specific designated material receiving area that is not adjacent to a vital area. Escort is not required for designated licensee vehicles or licensee-owned or leased vehicles entering the protected area and driven by personnel having unescorted access. Designated licensee vehicles shall be limited in their use to onsite plant functions and shall remain in the protected area except for operational, maintenance, repair, security, and emergency purposes. The licensee shall exercise positive control over all such designated vehicles to assure that they are used only by authorized persons and for authorized purposes.

(5)(i) A numbered picture badge identification system must be used for all individuals who are authorized access to protected areas without escort. An individual not employed by the licensee but who requires frequent and extended access to protected and vital areas may be authorized access to such areas without escort provided that he or she displays a licensee-issued picture badge upon entrance into the protected area which indicates:

- (A) Non-employee no escort required;
- (B) Areas to which access is authorized; and
- (C) The period for which access has been authorized.

(ii) Badges shall be displayed by all individuals while inside the protected area. Badges may be removed from the protected area when measures are in place to confirm the true identity and authorization for access of the badge holder upon entry to the protected area.

(6) Individuals not authorized by the licensee to enter protected areas without escort shall be escorted by a watchman or other individual designated by the licensee while in a protected area and shall be badged to indicate that an escort is required. In addition, the licensee shall require that each individual register his or her name, date, time,

purpose of visit, employment affiliation, citizenship, and name of the individual to be visited. The licensee shall retain the register of information for three years after the last entry in the register.

(7) The licensee shall:

(i) Establish an access authorization system to limit unescorted access to vital areas during nonemergency conditions to individuals who require access in order to perform their duties. To achieve this, the licensee shall:

(A) Establish a current authorization access list for all vital areas. The access list must be updated by the cognizant licensee manager or supervisor at least once every 31 days and must be reapproved at least quarterly. The licensee shall include on the access list only individuals whose specific duties require access to vital areas during nonemergency conditions.

(B) Positively control, in accordance with the access list established pursuant to paragraph (d)(7)(i) of this section, all points of personnel and vehicle access to vital areas.

(C) Revoke, in the case of an individual's involuntary termination for cause, the individual's unescorted facility access and retrieve his or her identification badge and other entry devices, as applicable, prior to or simultaneously with notifying this individual of his or her termination.

(D) Lock and protect by an activated intrusion alarm system all unoccupied vital areas.

(ii) Design the access authorization system to accommodate the potential need for rapid ingress or egress of individuals during emergency conditions or situations that could lead to emergency conditions. To help assure this, the licensee shall:

(A) Ensure prompt access to vital equipment.

(B) Periodically review physical security plans and contingency plans and procedures to evaluate their potential impact on plant and personnel safety.

(8) All keys, locks, combinations, and related access control devices used to control access to protected areas must be controlled to reduce the probability of compromise. Whenever there is evidence or suspicion that any key, lock, combination, or related access control devices may have been compromised, it must be changed or rotated. The licensee shall issue keys, locks, combinations and other access control devices to protected areas and vital areas only to persons granted unescorted facility access. Whenever an individual's unescorted access is revoked due to his or her lack of trustworthiness, reliability, or inadequate work performance, key, locks, combinations, and related access control devices to which that person had access, must be changed or rotated.

(e) Detection aids. (1) All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm. The onsite central alarm station must be considered a vital area and its walls, doors, ceiling, floor, and any windows in the walls and in the doors must be bullet-resisting. The onsite central alarm station must be located within a building in such a manner that the interior of the central alarm station is not visible from the

perimeter of the protected area. This station must not contain any operational activities that would interfere with the execution of the alarm response function. Onsite secondary power supply systems for alarm annunciator equipment and non-portable communications equipment as required in paragraph (f) of this section must be located within vital areas.

(2) All alarm devices including transmission lines to annunciators shall be tamper indicating and self-checking e.g., an automatic indication is provided when failure of the alarm system or a component occurs, or when the system is on standby power. The annunciation of an alarm at the alarm stations shall indicate the type of alarm (e.g., intrusion alarms, emergency exit alarm, etc.) and location.

(3) All emergency exits in each protected area and each vital area shall be alarmed.

(f) Communication requirements. (1) Each guard, watchman or armed response individual on duty shall be capable of maintaining continuous communication with an individual in each continuously manned alarm station required by paragraph (e)(1) of this section, who shall be capable of calling for assistance from other guards, watchmen, and armed response personnel and from local law enforcement authorities.

(2) The alarm stations required by paragraph (e)(1) of this section shall have conventional telephone service for communication with the law enforcement authorities as described in paragraph (f)(1) of this section.

(3) To provide the capability of continuous communication, radio or microwave transmitted two-way voice communication, either directly or through an intermediary, shall be established, in addition to conventional telephone service, between local law enforcement authorities and the facility and shall terminate in each continuously manned alarm station required by paragraph (e)(1) of this section.

(4) Non-portable communications equipment controlled by the licensee and required by this section shall remain operable from independent power sources in the event of the loss of normal power.

(g) Testing and maintenance. Each licensee shall test and maintain intrusion alarms, emergency alarms, communications equipment, physical barriers, and other security related devices or equipment utilized pursuant to this section as follows:

(1) All alarms, communication equipment, physical barriers, and other security related devices or equipment shall be maintained in operable condition. The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures.

(2) Each intrusion alarm shall be tested for performance at the beginning and end of any period that it is used for security. If the period of continuous use is longer than seven days, the intrusion alarm shall also be tested at least once every seven (7) days.

(3) Communications equipment required for communications onsite shall be tested for performance not less frequently than once at the beginning of each security personnel work shift. Communications equipment required for communications offsite shall be tested for performance not less than once a day.

(4)(i) The licensee shall review implementation of the security program by individuals who have no direct responsibility for the security program either:

(A) At intervals not to exceed 12 months, or

(B) As necessary, based on an assessment by the licensee against performance indicators and as soon as reasonably practicable after a change occurs in personnel, procedures, equipment, or facilities that potentially could adversely affect security but no longer than 12 months after the change. In any case, each element of the security program must be reviewed at least every 24 months.

(ii) 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 authorities. The results and recommendations of the security program review, management's findings on whether the security program is currently effective, 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 the day-to-day plant operation. These reports must be maintained in an auditable form, available for inspection, for a period of 3 years.

(h) Response requirement. (1) The licensee shall establish, maintain, and follow an NRC-approved safeguards contingency plan for responding to threats, thefts, and radiological sabotage related to the nuclear facilities subject to the provisions of this section. Safeguards contingency plans must be in accordance with the criteria in appendix C to this part, "Licensee Safeguards Contingency Plans."

(2) The licensee shall establish and document liaison with local law enforcement authorities. The licensee shall retain documentation of the current liaison as a record until the Commission terminates each license for which the liaison was developed and, if any portion of the liaison documentation is superseded, retain the superseded material for three years after each change.

(3) The total number of guards, and armed, trained personnel immediately available at the facility to fulfill these response requirements shall nominally be ten (10), unless specifically required otherwise on a case by case basis by the Commission; however, this number may not be reduced to less than five (5) guards.

(4) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, material access area, or a vital area; or upon evidence or indication of intrusion into a protected area, a material access area, or a vital area, the licensee security organization shall:

(i) Determine whether or not a threat exists,

(ii) Assess the extent of the threat, if any,

(iii) 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 material access areas and any adversary attempting entry for the purpose of radiological sabotage or theft of special nuclear material and to intercept any person exiting with special nuclear material, and,

(B) Informing local law enforcement agencies of the threat and requesting assistance.

(5) The licensee shall instruct every guard and all armed response personnel to prevent or impede attempted acts of theft or radiological sabotage by using force

sufficient to counter the force directed at him including the use of deadly force when the guard or other armed response person has a reasonable belief it is necessary in self-defense or in the defense of others.

(6) To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided, preferably by means of closed circuit television or by other suitable means which limit exposure of responding personnel to possible attack.

(Sec. 161i, Pub. L. 83-703, 68 Stat. 948, Pub. L. 93-377, 88 Stat. 475; secs. 201, 204(b)(1), Pub. L. 93-438, 88 Stat. 1242-1243, 1245, Pub. L. 94-79, 89 Stat. 413 (42 U.S.C. 2201, 5841))

[42 FR 10838, Feb. 24, 1977, as amended at 42 FR 51607, Sept. 29, 1977; 43 FR 11965, Mar. 23, 1978; 43 FR 34766, Aug. 7, 1978; 44 FR 65970, Nov. 16, 1979; 44 FR 68198, Nov. 28, 1979; 45 FR 79410, Dec. 1, 1980; 45 FR 83196, Dec. 18, 1980; 51 FR 27821, 27825, Aug. 4, 1986; 51 FR 30054, Aug. 22, 1986; 52 FR 12365, Apr. 16, 1987; 53 FR 19259, May 27, 1988; 57 FR 33431, July 29, 1992; 59 FR 38900, Aug. 1, 1994; 60 FR 46498, Sept. 7, 1995; 62 FR 63643, Dec. 2, 1997; 64 FR 14818, Mar. 29, 1999; 64 FR 17947, Apr. 13, 1999]