each general and specific licensee using its cask design.

(d) The updated FSAR shall be retained by the certificate holder until the Commission terminates the certificate.

(e) A certificate holder who permanently ceases operation, shall provide the updated FSAR to the new certificate holder or to the Commission, as appropriate, in accordance with §72.234(d)(3).

[64 FR 53617, Oct. 4, 1999, as amended at 68 FR 58819, Oct. 10, 2003; 74 FR 62684, Dec. 1, 2009]

PART 73—PHYSICAL PROTECTION OF PLANTS AND MATERIALS

Subpart A—General Provisions

Subpart B—Enhanced Weapons, Preemption, and Firearms Background Checks

Subpart C—General Performance Objective for Protection of Strategic Special Nuclear Material

Subpart D—Protection of Safeguards Information

Subpart E—Physical Protection Requirements of Special Nuclear Material and Spent Nuclear Fuel in Transit

Subpart F—Physical Protection Requirements at Fixed Sites

Subpart G—Access Authorization and Access Control Requirements for the Physical Protection of Special Nuclear Material

special nuclear material of moderate and low strategic significance.

Subpart H—Records and Postings

Subparts J–S—[Reserved]

Subpart T—Security Notifications, Reports, and Recordkeeping

AUTHORITY: Atomic Energy Act of 1954, secs. 53, 147, 149, 161, 161A, 170D, 170E, 170H, 170I, 223, 229, 234, 1701 (42 U.S.C. 2073, 2167, 2169, 2201, 2201a, 2210d, 2210e, 2210h, 2210i, 2273, 2278a, 2282, 2297f); Energy Reorganization Act of 1974, secs. 201, 202 (42 U.S.C. 5841, 5842); Nuclear Waste Policy Act of 1982, secs. 135, 141 (42 U.S.C. 10155, 10161); 44 U.S.C. 3504 note.

Section 73.37(b)(2) also issued under Sec. 301, Public Law 96–295, 94 Stat. 789 (42 U.S.C. 5841 note).

SOURCE: 38 FR 35430, Dec. 28, 1973, unless otherwise noted.

Subpart A—General Provisions

§ 73.1 Purpose and scope.

(a) *Purpose.* This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material. Licensees subject to the provisions of § 73.20 (except for fuel cycle licensees authorized under Part 70 of this chapter to receive, acquire, possess, transfer, use, or deliver for transportation formula quantities of strategic special nuclear material), §§ 73.50, and 73.60 are exempt from §§ 73.1(a)(1)(i)(E), 73.1(a)(1)(iii), 73.1(a)(1)(iv), 73.1(a)(2)(iii), and 73.1(a)(2)(iv). Licensees subject to the provisions of § 72.212 are exempt from § 73.1(a)(1)(iv).

(1) *Radiological sabotage.* (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes: A single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including handheld automatic weapons, equipped with silencers and having effective long range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system; and

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack.

(2) *Theft or diversion of formula quantities of strategic special nuclear material.* (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or individuals attacking through multiple entry points, or individuals attacking through separate entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including handheld automatic weapons, equipped with silencers and having effective long-range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safe-guards system;

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack.

(b) *Scope.* (1) This part prescribes requirements for:

(i) The physical protection of production and utilization facilities licensed under parts 50 or 52 of this chapter,

(ii) The physical protection of plants in which activities licensed pursuant to part 70 of this chapter are conducted, and

(iii) The physical protection of special nuclear material by any person who, pursuant to the regulations in part 61 or 70 of this chapter, possesses or uses at any site or contiguous sites subject to the control by the licensee, formula quantities of strategic special nuclear material or special nuclear material of moderate strategic significance or special nuclear material of low strategic significance.

(2) This part prescribes requirements for the physical protection of special nuclear material in transportation by any person who is licensed pursuant to the regulations in parts 70 and 110 of this chapter who imports, exports, transports, delivers to a carrier for transport in a single shipment, or takes delivery of a single shipment free on board (F.O.B.) where it is delivered to a carrier, formula quantities of strategic special nuclear material, special nuclear material of moderate strategic significance or special nuclear material of low strategic significance.

(3) This part also applies to shipments by air of special nuclear material in quantities exceeding: (i) 20 grams or 20 curies, whichever is less, of

plutonium or uranium-233, or (ii) 350 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U–235 isotope).

(4) Special nuclear material subject to this part may also be protected pursuant to security procedures prescribed by the Commission or another Government agency for the protection of classified materials. The provisions and requirements of this part are in addition to, and not in substitution for, any such security procedures. Compliance with the requirements of this part does not relieve any licensee from any requirement or obligation to protect special nuclear material pursuant to security procedures prescribed by the Commission or other Government agency for the protection of classified materials.

(5) This part also applies to the shipment of irradiated reactor fuel in quantities that in a single shipment both exceed 100 grams in net weight of irradiated fuel, exclusive of cladding or other structural or packaging material, and have a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surface without intervening shielding.

(6) This part prescribes requirements for the physical protection of spent nuclear fuel and high-level radioactive waste stored in either an independent spent fuel storage installation (ISFSI) or a monitored retrievable storage (MRS) installation licensed under part 72 of this chapter, or stored at the geologic repository operations area licensed under part 60 or part 63 of this chapter.

(7) This part prescribes requirements for the protection of Safeguards Information (including Safeguards Information with the designation or marking: Safeguards Information—Modified Handling) in the hands of any person, whether or not a licensee of the Commission, who produces, receives, or acquires that information.

(8) This part prescribes requirements for advance notice of export and import shipments of special nuclear material, including irradiated reactor fuel.

(9) As provided in part 76 of this chapter, the regulations of this part establish procedures and criteria for physical security for the issuance of a certificate of compliance or the approval of a compliance plan.

[44 FR 68186, Nov. 28, 1979]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 73.1, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at *www.govinfo.gov*.

§ 73.2 Definitions.

As used in this part:

(a) Terms defined in parts 50, 52, 70, and 95 of this chapter have the same meaning when used in this part.

Adverse firearms background check means a firearms background check that has resulted in a ''denied'' or ''delayed'' NICS response from the Federal Bureau of Investigation (FBI).

Appropriate Nuclear Regulatory Commission Regional Office listed in appendix A means:

(1) For domestic shipments—the Regional Office within whose region the licensee who is responsible for the physical protection arrangements of the shipment is located.

(2) For export shipments—the Regional Office within whose region the licensee who is responsible for the physical protection arrangements of the shipment is located, and the Regional Office for the region in which the last point of exit of the shipment from the U.S. is located.

(3) For import shipments—the Regional Office within whose region the licensee who is responsible for the physical protection arrangements of the shipment is located, and the Regional Office for the region in which the first point of entry of the shipment into the U.S. is located.

Armed escort means an armed person, not necessarily uniformed, whose primary duty is to accompany shipments of special nuclear material for the protection of such shipments against theft or radiological sabotage.

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

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

Background check includes, at a minimum, a Federal Bureau of Investigation (FBI) criminal history records check (including verification of identity based on fingerprinting), employment history, education, and personal references. Individuals engaged in activities subject to regulation by the Commission, applicants for licenses to engage in Commission-regulated activities, and individuals who have notified the Commission in writing of an intent to file an application for licensing, certification, permitting, or approval of a product or activity subject to regulation by the Commission are required under §73.57 to conduct fingerprinting and criminal history records checks before granting access to Safeguards Information. A background check must be sufficient to support the trustworthiness and reliability determination so that the person performing the check and the Commission have assurance that granting individuals access to Safeguards Information does not constitute an unreasonable risk to the public health and safety or the common defense and security.

Bullet/resisting means protection against complete penetration, passage of fragments of projectiles, and spalling (fragmentation) of the protective material that could cause injury to a person standing directly behind the bullet-resisting barrier.

Combined preemption authority and enhanced weapons authority means the authority granted to the Commission, pursuant to 42 U.S.C. 2201a, to authorize licensees or the designated security personnel of a licensee to transfer, receive, possess, transport, import, and use one or more categories of enhanced weapons, notwithstanding any State, local, or certain Federal firearms laws, including regulations, that prohibit or restrict such conduct.

Contiguous sites means licensee controlled locations, deemed by the Commission to be in close enough proximity to each other, that the special nuclear material must be considered in the aggregate for the purpose of physical protection.

Continuous visual surveillance means unobstructed view at all times of a shipment of special nuclear material, and of all access to a temporary storage area or cargo compartment containing the shipment.

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

Contraband means unauthorized firearms, explosives, incendiaries, or other dangerous materials (e.g., disease causing agents), which are capable of causing acts of sabotage against a licensed facility or licensed radioactive material, as specified under 42 U.S.C. 2284. For licensees that possess or conduct activities involving classified national security information or classified Restricted Data (RD) as defined in §95.5 of this chapter, contraband also means unauthorized electronic devices or unauthorized electronic media that are capable of facilitating acts of espionage; unauthorized communication, transmission, disclosure, or receipt of RD; or tampering with RD, pursuant to 18 U.S.C. 793 or 42 U.S.C. 2274–2276, respectively. Contraband items are banned from a licensee's protected area, vital area, materials access area, or controlled access area.

Covered weapon means any handgun, rifle, shotgun, short-barreled shotgun, short-barreled rifle, semiautomatic assault weapon, machine gun, ammunition for any such weapons, or large capacity ammunition feeding device otherwise prohibited by State, local, or certain Federal firearms laws, including regulations, as specified under 42 U.S.C. 2201a(b).

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

DOE and *Department of Energy* means the Department of Energy established by the Department of Energy Organization Act (Pub. L. 95–91, 91 Stat. 565, 42 U.S.C. 7101 *et seq.*), to the extent that the Department, or its duly authorized representatives, exercises functions formerly vested in the U.S. Atomic Energy Commission, its Chairman, members, officers and components and transfered to the U.S. Energy Research and Development Administration and to the Administrator thereof pursuant to sections 104(b), (c) and (d) of the Energy Reorganization Act of 1974 (Pub. L. 93–438, 88 Stat. 1233 at 1237, 42 U.S.C. 5814) and retransferred to the Secretary of Energy pursuant to section 301(a) of the Department of Energy Organization Act (Pub. L. 95–91, 91 Stat. 565 at 577–578, 42 U.S.C. 7151).

Enhanced weapon means any short-barreled shotgun, short-barreled rifle, or machine gun. Enhanced weapons do not include destructive devices as defined in 18 U.S.C. 921(a).

Enhanced weapon means any short-barreled shotgun, short-barreled rifle, or machine gun. Enhanced weapons do not include destructive devices as defined in 18 U.S.C. 921(a).

Firearms background check means a background check by the U.S. Attorney General pursuant to 42 U.S.C. 2201a that includes a check against the Federal Bureau of Investigation's (FBI's) fingerprint system and the National Instant Criminal Background Check System.

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

Formula quantity means strategic special nuclear material in any combination in a quantity of 5,000 grams or more computed by the formula, grams = (grams contained U-235) + 2.5 (grams U-233 + grams plutonium). This class of material is sometimes referred to as a Category I quantity of material.

Greater than Class C waste or *GTCC waste* has the same meaning as defined in § 72.3 of this chapter.

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

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

High-level radioactive waste or HLW has the same meaning as defined in § 72.3 of this chapter.

Independent spent fuel storage installation or ISFSI has the same meaning as defined in § 72.3 of this chapter.

Indian Tribe means an Indian or Alaska Native Tribe, band, nation, pueblo, village, or community that the Secretary of the Interior acknowledges to exist as an Indian Tribe pursuant to the Federally Recognized Indian Tribe List Act of 1994, 25 U.S.C. 5130.

Individual authorized access to Safeguards Information is an individual authorized to have access to and handle such information pursuant to the requirements of §§ 73.21 and 73.22 of this part.

Individual authorized access to Safeguards Information—Modified Handling is an individual authorized to have access to and handle Safeguards Information designated as Safeguards Information—Modified Handling information pursuant to the requirements of §§ 73.21 and 73.23 of this part.

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

Isolation zone means any area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual.

Lock in the case of vaults or vault type rooms means a three-position, manipulation resistant, dial type, built-in combination lock or combination padlock and in the case of fences, walls, and buildings means an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock. *Lock* in the case of a vault or vault type room also means any manipulation resistant,

electromechanical device which provides the same function as a built-in combination lock or combination padlock, which can be operated remotely or by the *reading* or insertion of information, which can be uniquely characterized, and which allows operation of the device. *Locked* means protected by an operable lock.

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

Movement control center means an operations center which is remote from the transport activity and which maintains position information on the movement of special nuclear material or radioactive material; receives reports of actual or attempted attacks, thefts, or sabotage; provides a means for notifying these and other problems to the NRC and appropriate agencies; and can request and coordinate appropriate aid.

Need to know means a determination by a person having responsibility for protecting Safeguards Information (including Safeguards Information designated as Safeguards Information—Modified Handling) that a proposed recipient's access to Safeguards Information is necessary in the performance of official, contractual, licensee, applicant, or certificate holder employment. In an adjudication, ''need to know'' means a determination by the originator of the information that the information is necessary to enable the proposed recipient to proffer and/or adjudicate a specific contention in that proceeding, and the proposed recipient of the specific Safeguards Information possesses demonstrable knowledge, skill, training, or education to effectively utilize the specific Safeguards Information in the proceeding. Where the information is in the possession of the originator and the NRC staff (dual possession), whether in its original form or incorporated into another document or other matter by the recipient, the NRC staff makes the determination. In the event of a dispute regarding the ''need to know'' determination, the presiding officer of the proceeding shall make the ''need to know'' determination.

NICS means the National Instant Criminal Background Check System established by Section 103(b) of the Brady Handgun Violence Prevention Act, Public Law 103–159 (107 Stat. 1536), that is operated by the FBI's Criminal Justice Information Services Division.

NICS response means a response provided by the FBI, as the result of a firearms background check against the NICS. A NICS response provided by the FBI may be ''proceed,'' ''delayed,'' or ''denied.''

NICS transaction number or *NTN* means the identification number created by the FBI to track firearms background checks upon entry of the information into the FBI's system. The NICS response and the NTN are the information returned by the FBI, following a firearms background check.

Person means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the Department of Energy (DOE), (except that the DOE shall be considered a person to the extent that its facilities are subject to the licensing and related regulatory authority of the Commission pursuant to section 202 of the Energy Reorganization Act of 1974 and sections 104, 105, and 202 of the Uranium Mill Tailings Radiation Control Act of 1978), any state or political subdivision of a state, or any political subdivision of any government or nation, or other entity; and (2) any legal successor, representative, agent, or agency of the foregoing.

Physical barrier means:

(1) Fences constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire or similar material on brackets angled inward or outward between 30° and 45° from the vertical, with an overall height of not less than eight feet, including the barbed topping;

(2) Building walls, ceilings and floors constructed of stone, brick, cinder block, concrete, steel or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or

walls of similar construction, not part of a building, provided with a barbed topping described in paragraph (1) of this definition of a height of not less than 8 feet; or

(3) Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.

Protected area means an area encompassed by physical barriers and to which access is controlled.

Radiological sabotage means any deliberate act directed against a plant or transport in which an activity licensed pursuant to the regulations in this chapter is conducted, or against a component of such a plant or transport which could directly or indirectly endanger the public health and safety by exposure to radiation.

Restricted Data or RD has the same meaning as defined in § 95.5 of this chapter.

Safeguards Information means information not classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed control and accounting procedures for the physical protection of special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; detailed security measures (including security plans, procedures, and equipment) for the physical protection of source, byproduct, or special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; security measures for the physical protection of and location of certain plant equipment vital to the safety of production or utilization facilities; and any other information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, the unauthorized disclosure of which, as determined by the Commission through order or regulation, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material.

Safeguards Information—Modified Handling is the designation or marking applied to Safeguards Information which the Commission has determined requires handling requirements modified from the specific Safeguards Information handling requirements that are applicable to Safeguards Information needing a higher level of protection.

Satisfactory firearms background check means a firearms background check that has resulted in a ''proceed'' NICS response.

Security management means persons responsible for security at the policy and general management level.

Security Storage Container includes any of the following repositories: (1) For storage in a building located within a protected or controlled access area, a steel filing cabinet equipped with a steel locking bar and a three position, changeable combination, GSA approved padlock; (2) A security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked, *General Services Administration Approved Security Container* on the exterior of the top drawer or door; (3) A bank safe-deposit box; and (4) Other repositories which in the judgement of the NRC, would provide comparable physical protection.

Security supervision means persons, not necessarily uniformed or armed, whose primary duties are supervision and direction of security at the day-to-day operating level.

Special nuclear material (SNM) has the same meaning as defined in § 70.4 of this chapter.

Special nuclear material of low strategic significance means:

(1) Less than an amount of special nuclear material of moderate strategic significance as defined in paragraph (1) of the definition of strategic nuclear material of moderate strategic significance in this section, but more than 15 grams of uranium-235 (contained in uranium enriched to 20 percent or more in U-235 isotope) or 15 grams of uranium-233 or 15 grams of plutonium or the combination of 15 grams when computed by the equation, grams = (grams

contained U-235) + (grams plutonium) + (grams U-233); or

(2) Less than 10,000 grams but more than 1,000 grams of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U-235 isotope); or

(3) 10,000 grams or more of uranium-235 (contained in uranium enriched above natural but less than 10 percent in the U-235 isotope).

This class of material is sometimes referred to as a Category III quantity of material.

Special nuclear material of moderate strategic significance means:

(1) Less than a formula quantity of strategic special nuclear material but more than 1,000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope) or more than 500 grams of uranium-233 or plutonium, or in a combined quantity of more than 1,000 grams when computed by the equation, grams = (grams contained U-235) + 2 (grams U-233 + grams plutonium); or

(2) 10,000 grams or more of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U-235 isotope).

This class of material is sometimes referred to as a Category II quantity of material.

Spent nuclear fuel (SNF) or spent fuel means the fuel that has been withdrawn from a nuclear reactor following irradiation and has not been chemically separated into its constituent elements by reprocessing. Spent nuclear fuel includes the special nuclear material, byproduct material, source material, and other radioactive materials associated with a fuel assembly.

Stand-alone preemption authority means the authority granted to the Commission, pursuant to 42 U.S.C. 2201a, to authorize licensees or the designated security personnel of a licensee to transfer, receive, possess, transport, import, and use one or more categories of covered weapons, notwithstanding any State, local, or certain Federal firearms laws, including regulations, that prohibit or restrict such conduct. Such covered weapons do not include enhanced weapons as defined in this part.

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

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

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

Time of discovery means the time at which a cognizant individual observes, identifies, or is notified of a security-significant event or condition. A cognizant individual is considered anyone who, by position, experience, and/or training, is expected to understand that a particular condition or event adversely impacts security.

Transport means any land, sea, or air conveyance or modules for these conveyances such as rail cars or standardized cargo containers.

Tribal official means the highest ranking individual that represents Tribal leadership, such as the Chief, President, or Tribal Council leadership.

Trustworthiness and reliability are characteristics of an individual considered dependable in judgment, character, and performance, such that disclosure of Safeguards Information (including Safeguards Information designated as Safeguards Information—Modified Handling) to that individual does not constitute an unreasonable risk to the public health and safety or common defense and security. A determination of trustworthiness and reliability for this purpose is based upon a background check.

Undergoing processing means performing active operations on material such as chemical transformation, physical transformation, or transit between such operations, to be differentiated from storage or packaging for shipment.

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

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

Vital area means any area which contains vital equipment.

Vital equipment means any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

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

(b) The terms ''ammunition,'' ''handgun,'' ''rifle,'' ''machine gun,'' ''large capacity ammunition feeding device,'' ''semiautomatic assault weapon,'' ''short-barreled shotgun,'' ''short-barreled rifle,'' and ''shotgun'' specified in §§ 73.15 and 73.17 have the same meaning as provided for these terms in the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives' regulations at 27 CFR 478.11.

(c) The terms ''delayed,'' ''denied,'' and ''proceed'' that are used in NICS responses specified in this section have the same meaning provided these terms in the FBI's regulations at 28 CFR 25.2.

[38 FR 35430, Dec. 28, 1973]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 73.2, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at *www.govinfo.gov*.

§ 73.3 Interpretations.

Except as specifically authorized by the Commission in writing, no interpretations of the meaning of the regulations in this part by any officer or employee of the Commission other than a written interpretation by the General Counsel will be recognized as binding upon the Commission.

§ 73.4 Communications.

Except where otherwise specified, all communications and reports concerning the regulations in this part and applications filed under them should be sent as follows:

(a) By mail addressed to: ATTN: Document Control Desk, Director, Office of Nuclear Reactor Regulation, Director, Office of Nuclear Material Safety and Safeguards, or Director, Office of Nuclear Security and Incident Response, as appropriate, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001;

(b) By hand delivery to the NRC's offices at 11555 Rockville Pike, Rockville, Maryland 20852–2783;

(c) Where practicable, by electronic submission, for example, Electronic Information Exchange, or CD-ROM. Electronic submissions must be made in a manner that enables the NRC to receive, read, authenticate, distribute, and archive the submission, and process and retrieve it a single page at a time. Detailed guidance on making electronic submissions can be obtained by visiting the NRC's Web site at *http://www.nrc.gov/site-help/e-submittals.html;* by e-mail to *MSHD.Resource@nrc.gov;* or by writing the Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. The guidance discusses, among other topics, the formats the NRC can accept, the use of electronic signatures, and the treatment of nonpublic information.

(d) Classified communications shall be transmitted to the NRC Headquarters' classified mailing address as specified in appendix A to part 73 of this chapter or delivered by hand in accordance with this paragraph.

[68 FR 58819, Oct. 10, 2003, as amended at 73 FR 5725, Jan. 31, 2008; 74 FR 62684, Dec. 1, 2009; 80 FR 74981, Dec. 1, 2015; 83 FR 58723, Nov. 21, 2018; 84 FR 65646, Nov. 29, 2019; 88 FR 57879, Aug. 24, 2023]

§ 73.5 Specific exemptions.

The Commission may, upon application of any interested person or upon

its own initiative, grant such exemptions from the requirements of the regulations in this part as it determines are authorized by law and will not endanger life or property or the common defense and security, and are otherwise in the public interest.

§ 73.6 Exemptions for certain quantities and kinds of special nuclear material.

A licensee is exempt from the requirements of 10 CFR part 26 and §§ 73.20, 73.25, 73.26, 73.27, 73.45, 73.46, 73.70 and 73.72 with respect to the following special nuclear material:

(a) Uranium-235 contained in uranium enriched to less than 20 percent in the U–235 isotope.

(b) Special nuclear material which is not readily separable from other radioactive material and which has a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surface without intervening shielding.

(c) Special nuclear material in a quantity not exceeding 350 grams of uranium-235, uranium-233, plutonium, or a combination thereof, possessed in any analytical, research, quality control, metallurgical or electronic laboratory.

(d) Special nuclear material that is being transported by the United States Department of Energy transport system.

(e) Special nuclear material at nonpower reactors.

Licensees subject to § 73.60 are not exempted from §§ 73.70 and 73.72, and licensees subject to § 73.67(e) are not exempted from § 73.72 of this part.

[40 FR 52841, Nov. 13, 1975, as amended at 44 FR 68187, Nov. 28, 1979; 58 FR 31471, June 3, 1993; 78 FR 34250, June 7, 2013; 86 FR 43402, Aug. 9, 2021]

§ 73.8 Information collection requirements: OMB approval.

(a) The Nuclear Regulatory Commission has submitted the information collection requirements contained in this part to the Office of Management and Budget (OMB) for approval as required by the Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*). The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information is it does not display a currently valid OMB control number. OMB has approved the information collection requirements contained in this part under control number 3150–0002.

(b) The approved information collection requirements contained in this part appear in §§ 73.5, 73.15, 73.17, 73.20, 73.21, 73.24, 73.25, 73.26, 73.27, 73.37, 73.40, 73.45, 73.46, 73.50, 73.54, 73.55, 73.56, 73.57, 73.58, 73.60, 73.67, 73.70, 73.72, 73.73, 73.74, 73.1200, 73.1205, 73.1210, 73.1215, and appendices B and C to this part.

(c) This part contains information collection requirements in addition to those approved under the control number specified in paragraph (a) of this section. These information collection requirements and control numbers under which they are approved are as follows:

(1) In § 73.17, NRC Form 754 is approved under control number 3150–0204;

(2) In §§ 73.17 and 73.57, Federal Bureau of Investigation Form FD–258 is approved under control number 1110–0046; and

(3) In § 73.1205, NRC Form 366 is approved under control number 3150–0104.

[62 FR 52189, Oct. 6, 1997, as amended at 67 FR 67101, Nov. 4, 2002; 73 FR 63574, Oct. 24, 2008; 74 FR 13970, Mar. 27, 2009; 77 FR 39909, July 6, 2012; 78 FR 29550, May 20, 2013; 80 FR 67275, Nov. 2, 2015; 80 FR 74981, Dec. 1, 2015; 88 FR 15882, Mar. 14, 2023]

Subpart B—Enhanced Weapons, Preemption, and Firearms Background Checks

SOURCE: 88 FR 15882, Mar. 14, 2023, unless otherwise noted.

§ 73.15 Authorization for use of enhanced weapons and preemption of firearms laws.

(a) *Purpose*. This section presents the requirements for licensees to obtain approval to use the authority provided to the Commission under Section 161A of the Atomic Energy Act of 1954, as amended (AEA), in protecting Commission-designated classes of facilities, radioactive material, or other property. This authority includes ''stand-alone preemption authority'' and ''combined preemption authority and enhanced weapons authority.''

(b) *General Requirements.* (1) Licensees of facilities, activities, and other property listed in paragraph (c) of this section may apply to the NRC, in accordance with the provisions of this section, to receive stand-alone preemption authority or combined preemption authority and enhanced weapons authority.

(2) With respect to the possession and use of firearms by all other NRC licensees, the Commission's requirements in effect before April 13, 2023 remain applicable, except to the extent that those requirements are modified by an NRC order or regulations applicable to these licensees.

(c) *Applicability.* (1) Stand-alone preemption authority. The license holders for the following classes of facilities, radioactive material, or other property are designated by the Commission as eligible to apply for stand-alone preemption authority pursuant to 42 U.S.C. 2201a—

(i) Nuclear power reactor facilities;

(ii) Facilities authorized to possess or use a formula quantity or greater of strategic special nuclear material, where the material has a radiation level less than or equal to 1 gray (Gy) (100 Rad) per hour at a distance of 1 meter (m) (3.3 feet (ft)), without regard to any intervening shielding;

(iii) Independent spent fuel storage installations; and

(iv) Spent nuclear fuel transportation.

(2) Combined preemption authority and enhanced weapons authority. The license holders for the following classes of facilities, radioactive material, or other property are designated by the Commission as eligible to apply for combined enhanced weapons authority and preemption authority pursuant to 42 U.S.C. 2201a—

(i) Nuclear power reactor facilities;

(ii) Facilities authorized to possess or use a formula quantity or greater of strategic special nuclear material, where the material has a radiation level less than or equal to 1 Gy (100 Rad) per hour at a distance of 1 m (3.3 ft), without regard to any intervening shielding;

(iii) Independent spent fuel storage installations; and

(iv) Spent nuclear fuel transportation.

(d) *Application process for stand-alone preemption authority.* (1) Only licensees included within the classes of facilities, radioactive material, and other property listed in paragraph (c)(1) of this section may apply to the NRC for stand-alone preemption authority.

(2) Licensees applying for stand-alone preemption authority must submit an application to the NRC using the procedures specified in this section.

(3) The contents of the application must include the following information:

(i) A statement indicating that the licensee is applying for stand-alone preemption authority;

(ii) The Commission-designated facility, radioactive material, or other property to be protected by the licensee's security personnel using the covered weapons;

(iii) A description of the licensee's purposes and objectives in requesting stand-alone preemption authority. This description must include whether these covered weapons are currently employed as part of the licensee's existing protective strategy or whether these covered weapons will be used in a revised protective strategy; and

(iv) A description of the licensee's Firearms Background Check Plan, as required by § 73.17 of this part.

(4) Once a licensee has been notified that its application for stand-alone preemption authority has been accepted for review by the NRC, the licensee must provide the following supplemental information once it becomes available:

(i) A confirmation that a sufficient number of security personnel have completed a satisfactory firearms background check to meet the licensee's security personnel minimum staffing requirements, as specified in its physical security plan and any applicable fatigue requirements under part 26 of this chapter;

(ii) A confirmation that the necessary training modules and notification procedures have been developed under its Firearms Background Check Plan; and

(iii) A confirmation that all security personnel whose official duties require

access to covered weapons have been trained on these modules and notification procedures.

(5) The licensee must submit both the application and the supplementary information to the NRC in writing, under oath or affirmation, and in accordance with § 73.4 of this part.

(6) Upon the effective date of the NRC's approval of its application for stand-alone preemption authority, the licensee must only assign security personnel who have completed a satisfactory firearms background check to duties requiring access to any covered weapons.

(e) *Application process for combined preemption authority and enhanced weapons authority.*

(1) Only licensees included within the classes of facilities, radioactive material, and other property listed in paragraph (c)(2) of this section may apply to the NRC for combined preemption authority and enhanced weapons authority.

(2) Licensees applying for combined preemption authority and enhanced weapons authority must submit an application to the NRC using the procedures specified in this section.

(3) The contents of the application must include the following information:

(i) A statement indicating that the licensee is applying for combined preemption authority and enhanced weapons authority;

(ii) The Commission-designated facility, radioactive material, or other property to be protected by the licensee's security personnel using the covered weapons, including enhanced weapons;

(iii) A description of the licensee's purposes and objectives in requesting combined preemption authority and enhanced weapons authority. This must include whether these enhanced weapons are currently employed as part of the licensee's existing protective strategy or whether these enhanced weapons will be used in a revised protective strategy;

(iv) The total quantities of enhanced weapons, including the types and calibers or gauges, requested; and

(v) A description of the licensee's Firearms Background Check Plan, required by § 73.17 of this part.

(vi) If the NRC has previously approved the licensee's application for stand-alone preemption authority under either paragraph (d) of this section or under an NRC Order issued before April 13, 2023, then the licensee must include the effective date of the NRC's approval for stand-alone preemption authority in its application for combined preemption authority and enhanced weapons.

(4) The licensee must include with its application the additional technical information required by paragraph (f) of this section.

(5) Once a licensee has been notified that its application for combined preemption authority and enhanced weapons authority has been accepted for review by the NRC, the licensee must provide the following supplemental information once it becomes available:

(i) A confirmation that a sufficient number of security personnel have completed a satisfactory firearms background check to meet the licensee's security personnel minimum staffing requirements, as specified in its physical security plan, and any applicable fatigue requirements under part 26 of this chapter;

(ii) A confirmation that the necessary training modules and notification procedures have been developed under its Firearms Background Check Plan; and

(iii) A confirmation that security personnel, whose official duties require access to enhanced weapons, have been trained on these modules and notification procedures.

(iv) Exceptions: Licensees that were previously approved by the NRC for stand-alone preemption authority do not have to submit the supplemental information required by paragraph (e)(5) since it has been previously submitted under paragraph (d)(4) of this section or in response to an NRC Order.

(6) The licensee must submit its application in accordance with the applicable license amendment provisions specified in § 50.90, § 70.34, or § 72.56 of this chapter. The licensee must submit both the application and the supplementary information to the NRC in

writing, under oath or affirmation, and in accordance with § 73.4 of this part.

(7) If a licensee wishes to use a different type or caliber or gauge of an enhanced weapon or obtain a different quantity of enhanced weapons from that previously approved by the Commission under this section, then the licensee must submit a new application to the NRC in accordance with paragraph (e) of this section (to address these different weapons or different quantities of weapons).

(8) Upon the effective date of the NRC's approval of its application for combined preemption authority and enhanced weapons authority, the licensee must only assign security personnel who have completed a satisfactory firearms background check to duties requiring access to any covered weapons.

(f) *Application for combined preemption authority and enhanced weapons authority additional technical information.* (1) A licensee must also submit to the NRC for prior review and approval the following plans and assessments. These plans and assessments must be specific to the facility, radioactive material, or other property being protected.

(i) A new or revised physical security plan, security personnel training and qualification plan, and safeguards contingency plan; and

(ii) A new weapons safety assessment.

(2) In addition to other requirements presented in this part, these plans and assessments must—

(i) For the physical security plan, identify the quantities, types, and calibers or gauges of enhanced weapons that will be deployed;

(ii) For the training and qualification plan, address the training and qualification requirements to use these specific enhanced weapons;

(iii) For the safeguards contingency plan—

(A) The licensee must address how these enhanced weapons will be employed by the security personnel in implementing the protective strategy, including tactical approaches and maneuvers;

(B) In such instances where the addition of the enhanced weapons would not affect the content of the safeguards contingency plan, the required information on how the weapons will be employed may instead be incorporated into the licensee's physical security plan or an addendum thereto;

(C) Furthermore, in such instances, the licensee's application shall indicate that the proposed enhanced weapons do not affect the content of the NRC-approved safeguards contingency plan and it remains unchanged; and

(iv) For the weapons safety assessment, assess any potential safety impact by the use of enhanced weapons—

(A) At the facility, radioactive material, or other property being protected;

(B) On public or private facilities, public or private property, or on members of the public in areas outside of the site boundary; and

(C) On public or private facilities, public or private property, or on members of the public from the use of these enhanced weapons at training facilities; and

(D) Such assessments must consider both accidental and deliberate discharge of the enhanced weapons. However, licensees are not required to assess malevolent discharges of these enhanced weapons by trained and qualified security personnel, who have been screened and evaluated by the licensee's insider mitigation or human reliability programs.

(3) The licensee's training and qualification plan for enhanced weapons must be based upon applicable firearms standards developed by nationally-recognized firearms organizations or standard setting bodies or from standards developed by—

(i) Federal agencies, such as the U.S. Department of Homeland Security's Federal Law Enforcement Training Center, the U.S. Department of Energy's National Training Center, and the U.S. Department of Defense;

(ii) State law-enforcement training centers; or

(iii) State Division (or Department) of Criminal Justice Services Training Academies.

(g) *Conditions of approval.* (1) Licensees that have been approved by the NRC for combined preemption authority and enhanced weapons authority

must provide a copy of the NRC's authorization to the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) Federal firearms license (FFL) holder (*i.e.*, the transferor) for inclusion with the application to request ATF's pre-approval of the transfer and registration of the enhanced weapons to the NRC licensee (*i.e.*, the transferee).

(2) Licensees receiving enhanced weapons must comply with applicable ATF regulations in 27 CFR part 479.

(3) All enhanced weapons possessed by the licensee must be registered under the name of the licensee. Enhanced weapons may not be registered under the name of a licensee's security contractor.

(4) Licensees obtaining enhanced weapons may, at their discretion, also apply to ATF to obtain an FFL or a special occupational tax stamp, in conjunction with obtaining these enhanced weapons.

(h) *Completion of training and qualification before deployment of enhanced weapons.* (1) Licensees that have received combined preemption authority and enhanced weapons authority must ensure that their security personnel with access to enhanced weapons have completed the required firearms training and qualification, in accordance with the licensee's training and qualification plan.

(2) Initial training and qualification on enhanced weapons must be completed before the security personnel's deployment of enhanced weapons to implement the licensee's protective strategy.

(3) Recurring training and qualification on enhanced weapons by security personnel must be completed in accordance with the licensee's training and qualification plan.

(4) All training must be documented in accordance with the requirements of the licensee's training and qualification plan.

(i) [Reserved]

(j) *Use of enhanced weapons.* The requirements regarding the use of force by the licensee's security personnel, in the performance of their official duties, are contained in §§ 73.46, 73.51, and 73.55 and in appendices B, C, and H of this part, as applicable.

(k) *Notification of adverse ATF findings.* Requirements on notification of adverse ATF inspection or enforcement findings can be found under § 73.1200 of this part.

(l) [Reserved]

(m) *Transfer of enhanced weapons.* (1)(i) A licensee's issuance of enhanced weapons to its security personnel is not considered a transfer of those weapons as specified under ATF's regulations in 27 CFR part 479, provided the enhanced weapons remain within the site of a facility.

(ii) Remaining within the site of a facility means within the site boundary, as defined by the licensee's safety analysis report submitted to the NRC.

(2) A licensee's issuance of enhanced weapons to its security personnel for the permissible reasons specified in paragraph (m)(3) of this section, for activities that are outside of the facility's site boundary, are not considered a transfer under the provisions of 26 U.S.C. chapter 53, as specified under ATF's regulations in 27 CFR part 479, provided—

(i) The security personnel possessing the enhanced weapons are employees of the licensee; or

(ii) The security personnel possessing the enhanced weapons are employees of a contractor providing security services to the licensee and these contractor security personnel are under the direction of, and accompanied by, an authorized licensee employee.

(3) Permissible reasons for removal of enhanced weapons from the licensee's facility include—

(i) Removal of enhanced weapons for use at a firing range or training facility that is used by the licensee in accordance with its NRC-approved training and qualification plan for enhanced weapons;

(ii) Removal of enhanced weapons for use in escorting shipments of radioactive material or other property designated under paragraph (c) of this section that are being transported to or from the licensee's facility; or

(iii) Removal of an enhanced weapon from a licensee's facility to a gunsmith for the purposes of repair or maintenance and the subsequent return of the enhanced weapon to the licensee's facility.

(4) A licensee that has authorized the removal of enhanced weapons from its facility for any of the permissible reasons listed under paragraph (m)(3) of this section must verify that these weapons are returned to the facility upon the completion of the authorized activity.

(5) Removal of enhanced weapons from and/or return of these weapons to the licensee's facility must be documented in accordance with the records requirements of paragraph (q) of this section.

(6) Removal of enhanced weapons from a licensee's facility for reasons other than those set forth in paragraph (m)(3) of this section are considered a transfer as specified under ATF's regulations in 27 CFR part 479.

(7) The licensee may only transfer enhanced weapons pursuant to an ATF application to transfer and register the weapons that is approved by ATF in advance of the transfer, as required by ATF's regulations under 27 CFR part 479. Examples of transfers include, but are not limited to:

(i) Sale or disposal of an enhanced weapon to another authorized NRC licensee;

(ii) Sale or disposal of an enhanced weapon to an authorized Federal firearms license holder, government agency, or official police organization; or

(iii) Abandonment of an enhanced weapon to ATF.

(8) Following the completion of their official duties, security personnel must either—

(i) Return issued enhanced weapons to a licensee's authorized enhanced weapons storage location, as specified in the licensee's physical security plan, or

(ii) Turn over responsibility for the issued enhanced weapon to another on-shift security personnel authorized to use enhanced weapons as part of their official duties.

(9) Enhanced weapons that are not returned to the licensee's facility, following permissible removal, must be considered a transfer of a weapon under this paragraph, or a stolen or lost weapon under paragraph (p) of this section, as applicable. Information on the transfer, theft, or loss of an enhanced weapon must be documented, as required under paragraph (q) of this section.

(n) *Transport of weapons.* (1) Security personnel transporting enhanced weapons to or from a firing range or training facility used by the licensee must ensure that these weapons are unloaded and locked in a secure container during transport. Unloaded weapons and ammunition may be transported in the same locked secure container.

(2) Security personnel transporting enhanced weapons to or from a licensee's facility following the completion of, or in preparation for, escorting shipments of radioactive material or other property must ensure that these weapons are unloaded and locked in a secure container during transport. Security personnel may transport unloaded weapons and ammunition in the same locked secure container.

(3) Security personnel using enhanced weapons to protect shipments of radioactive material or other property that are being transported to or from the licensee's facility must ensure that these weapons are maintained in a state of loaded readiness and available for immediate use, except when otherwise prohibited by 18 U.S.C. 922(q).

(4) Security personnel transporting enhanced weapons to or from the licensee's facility must also comply with the requirements of § 73.17 of this part.

(5) Situations where security personnel transport enhanced weapons to or from the licensee's facility are not considered transfers of these weapons under ATF's regulations in 27 CFR part 479, provided—

(i) The security personnel transporting the enhanced weapons are employees of the licensee; or

(ii) The security personnel transporting the enhanced weapons are employees of a contractor providing security services to the licensee; and these contractor security personnel are under the direction of, and accompanied by, an authorized licensee employee.

(6) For the interstate transportation of enhanced weapons, pursuant to this section, the licensee must obtain prior written approval from ATF, as required by 27 CFR part 478.

(o) *Periodic inventories of enhanced weapons.* (1) Licensees possessing enhanced weapons under this section must conduct the following periodic accountability inventories of the enhanced weapons in their possession to verify the continued presence of each enhanced weapon that the licensee is authorized to possess.

(2)(i) Licensees must conduct a monthly inventory to verify that the authorized quantity of enhanced weapons are present at the licensee's facility.

(ii) Licensees must verify the presence of each individual enhanced weapon.

(iii) Licensees that store enhanced weapons in a locked secure weapons container (e.g., a ready-service arms locker) located within a protected area, vital area, or material access area may verify the presence of an intact tamper-indicating device (TID) on the locked secure weapons container, instead of verifying the presence of each individual weapon.

(iv) Verification of the presence of enhanced weapons via the presence of an intact TID must be documented in the inventory records and include the serial number of the TID.

(v) Licensees may use electronic technology (e.g., bar-codes on the weapons) in conducting such inventories.

(vi) The time interval from the previous monthly inventory must not exceed 30 + 7 days.

(3)(i) Licensees must conduct an annual inventory to verify that each authorized enhanced weapon is present at the licensee's facility through the verification of the serial number of each enhanced weapon.

(ii) Licensees must verify the presence of each enhanced weapon located in a locked secure weapons container (e.g., a ready-service arms locker) through the verification of the serial number of each enhanced weapon located within the container.

(iii) The time interval from the previous annual inventory must not exceed 365 + 7 days.

(iv) Licensees conducting an annual inventory may substitute this annual inventory in lieu of conducting the normal monthly inventory for that particular month, as required under paragraph (o) of this section.

(4) Licensees must conduct periodic inventories of enhanced weapons using either a two-person team or a single individual, provided the individual is subject to the licensee's behavioral observation or human reliability programs.

(5) The results of any periodic inventories of enhanced weapons must be retained in accordance with the records requirements of paragraph (q) of this section.

(6) Licensees must inventory any locked secure weapons container that was sealed with a TID and has subsequently been opened and must verify the serial number for each of the enhanced weapons stored in the weapons container. The inventoried weapons container must be relocked and resealed with a new TID and the new TID's serial number must be recorded in the periodic inventory records. The inventory must be conducted in accordance with the requirements of paragraph (o)(4) of this section.

(i) Licensees must use TIDs with unique serial numbers on locked secure weapons containers containing enhanced weapons.

(ii) Licensees must store unused TIDs in a manner similar to other security access control devices (e.g., keys, lock cores, etc.) and must maintain a log of issued TID serial numbers.

(7) Licensees must resolve any discrepancies identified during periodic inventories within 24 hours of their identification; otherwise, the discrepancy must be treated as a stolen or lost enhanced weapon and notifications must be made in accordance with paragraph (p) of this section.

(8) As an exception, enhanced weapons that are offsite for authorized purposes, in accordance with paragraphs (m) and (n) of this section, are required to be included in a periodic inventory but are not considered lost or stolen solely because they are offsite. The licensee must document the absence of these weapon(s) from the licensee's facility in the report of the results of a completed periodic enhanced weapons inventory, as required under paragraph (q) of this section.

(p) *Stolen or lost enhanced weapons.* (1) Licensees that discover that any enhanced weapons they are authorized to possess under this section are stolen or lost, must notify the NRC and local law enforcement officials in accordance with § 73.1200 of this part.

(2) Licensees that discover that any enhanced weapons they are authorized to possess under this section are stolen or lost are also required to notify ATF in accordance with ATF's regulations in 27 CFR part 479.

(q) *Records requirements.* (1) Licensees possessing enhanced weapons under this section must maintain records relating to the receipt, transfer, transportation, and inventory of such enhanced weapons.

(2) Licensees must maintain the following minimum records regarding the receipt of each enhanced weapon, including—

(i) Date of receipt of the weapon;

(ii) Name and address of the transferor who transferred the weapon to the licensee;

(iii) Name of the manufacturer of the weapon, or the name of the importer (for weapons manufactured outside the U.S.); and

(iv) Serial number, type, and caliber or gauge of the weapon.

(3) Licensees must maintain the following minimum records regarding the transfer of each enhanced weapon—

(i) Date of shipment of the weapon;

(ii) Name and address of the transferee who received the weapon; and

(iii) Serial number, type, and caliber or gauge of the weapon.

(4) Licensees must maintain the following minimum records regarding the transportation of each enhanced weapon away from the licensee's facility—

(i) Date of departure of the weapon;

(ii) Date of return of the weapon;

(iii) Purpose of the weapon's removal from the facility;

(iv) Name(s) of the security personnel transporting the weapon;

(v) Name(s) of the licensee employee accompanying and directing the transportation, where the security personnel transporting the weapons are employees of a security contractor providing security services to the licensee;

(vi) Name of the person/facility to whom the weapon is being transported; and

(vii) Serial number, type, and caliber or gauge of the weapon.

(5) Licensees possessing enhanced weapons pursuant to this section must document in these records the discovery that any of these enhanced weapons are stolen or lost.

(6) Licensees possessing enhanced weapons pursuant to this section must maintain records relating to the inventories of enhanced weapons for a period of up to one year after the licensee's authority to possess enhanced weapons is terminated, suspended, or revoked under paragraph (r) of this section and all enhanced weapons have been transferred from the licensee's facility.

(7) Licensees may integrate any records required by this section with records maintained by the licensee pursuant to ATF's regulations.

(8) Licensees must make any records required by this section available to NRC staff and ATF staff upon request.

(r) *Termination, modification, suspension, or revocation of Section 161A authority.*

(1)(i) Licensees seeking to terminate their stand-alone preemption authority must apply to the NRC in writing, under oath or affirmation, and in accordance with § 73.4.

(ii) Licensees seeking to terminate their combined enhanced weapons authority and preemption authority must apply to the NRC in writing, under oath or affirmation, and in accordance with § 73.4, and the license amendment provisions of § 50.90, § 70.34, or § 72.56 of this chapter, as applicable. These licensees must have transferred or disposed of any enhanced weapons, in accordance with the provisions of paragraph (m) of this section, prior to the NRC approval of a request for termination of their authority.

(2) Licensees seeking to modify their combined preemption authority and enhanced weapons authority, issued under this section, must apply to the NRC in writing, under oath or affirmation, and in accordance with § 73.4, and the license amendment provisions of § 50.90, § 70.34, or § 72.56 of this chapter, as applicable. Licensees' applications

to modify their enhanced weapons authority must provide the information required under paragraphs (e) and (f) of this section.

(i) Licensees seeking to replace their enhanced weapons with different types of enhanced weapons must amend their original application to include the different quantities, types, and calibers or gauges of the new enhanced weapons. This amended application must include a plan to transfer or dispose of their existing enhanced weapons once the new weapons are deployed.

(ii) Licensees adding additional quantities or types of enhanced weapons do not require a transfer or disposal plan.

(3) The Commission may revoke, suspend, or modify, in whole or in part, any approval issued under this section for any material false statement in the application or other statement of fact required of the licensee; or because of conditions revealed by the application or statement of fact or any report, record, inspection, or other means that would warrant the Commission refusing to grant approval of an original application; or for violation of, or for failure to observe, any of the terms and provisions of the act, regulations, license, permit, approval, or order of the Commission, or for any other reason that the Commission determines is appropriate.

(4) Licensees that have their stand-alone preemption authority or combined preemption authority and enhanced weapons authority terminated, suspended, or revoked may reapply for such authority by filing a new application under the provisions of this section.

(5) The NRC will notify ATF within 3 business days after taking action to terminate, modify, suspend, or revoke a licensee's stand-alone preemption authority or combined preemption authority and enhanced weapons authority issued under this section.

(s) *Withdrawal of orders.* For licensees that received an order issued under Section 161A (42 U.S.C. 2201a) prior to April 13, 2023, the following provisions apply.

(1) Licensees are not required to reapply for this authority.

(2) The requirements of such orders are superseded in their entirety by the requirements of this section and § 73.17 of this part.

(3) Licensees must complete their transition from the confirmatory orders to the requirements of this rule by January 8, 2024.

(4) On January 8, 2024 the following orders are withdrawn:

(i) Order EA–13–092, ''Order Designating an Interim Class of NRC-Licensed Facilities that are Eligible to Apply to the Commission for Authorization to Use the Authority Granted Under the Provisions of Section 161a of the Atomic Energy Act of 1954, as Amended'' (78 FR 35984; June 14, 2013);

(ii) Confirmatory Order EA–15–006, ''In the Matter of BWXT Nuclear Operations Group, Inc.'' (80 FR 53588; September 4, 2015);

(iii) Confirmatory Orders EA–14–135 and EA–14–136, ''In the Matter of Entergy Nuclear Operations Inc.; Entergy Nuclear Indian Point 2, LLC; and Entergy Nuclear Indian Point 3, LLC (Indian Point Nuclear Generating Unit (Nos. 1, 2, and 3)'' (81 FR 2247; January 15, 2016);

(iv) Confirmatory Order EA–14–137, ''In the Matter of Entergy Nuclear Fitzpatrick, LLC and Entergy Nuclear Operations Inc. (James A. Fitzpatrick Nuclear Power Plant)'' (81 FR 2247; January 15, 2016);

(v) Confirmatory Order EA–14–138, ''In the Matter of Exelon Generation Company, LLC (Nine Mile Point Nuclear Station Units 1 and 2)'' (81 FR 2247; January 15, 2016);

(vi) Confirmatory Order EA–14–139, ''In the Matter of Exelon Generation Company, LLC (R.E. Ginna Nuclear Power Plant)'' (81 FR 2247; January 15, 2016);

(vii) Confirmatory Order EA–14–134, ''In the Matter of Pacific Gas and Electric Company (Diablo Canyon Nuclear Power Plant, Units 1 and 2, and DCPP Independent Spent Fuel Storage Installation)'' (81 FR 2247; January 15, 2016); and

(viii) Confirmatory Order EA–14–140, ''In the Mater of Southern California Edison Company (San Onofre Nuclear Generating Station, Units 2 and 3, and Independent Spent Fuel Storage Installation)'' (81 FR 2247; January 15, 2016).

§ 73.17 Firearms background checks for armed security personnel.

(a) *Purpose.* This section presents the requirements for completion of firearms background checks pursuant to Section 161A of the Atomic Energy Act, as amended (AEA) (42 U.S.C. 2201a), for security personnel whose official duties require access to covered weapons at Commission-designated classes of facilities, radioactive material, or other property specified in § 73.15(c). Firearms background checks are intended to verify that such armed security personnel are not prohibited from receiving, possessing, transporting, importing, or using covered weapons under applicable Federal, State, or local law.

(b) *General Requirements.* (1) Licensees that have applied to the NRC under § 73.15 of this part for stand-alone preemption authority or for combined preemption authority and enhanced weapons authority must comply with the provisions of this section. Such licensees must establish a Firearms Background Check Plan. Licensees must establish this plan as part of their overall NRC-approved Training and Qualification plan for security personnel whose official duties require access to covered weapons.

(2) For the purposes of § 73.15 and this section only, the term security personnel whose official duties require access to covered weapons includes, but is not limited to, the following groups of individuals:

(i) Security officers using covered weapons to protect a Commission-designated facility, radioactive material, or other property;

(ii) Security officers undergoing firearms training on covered weapons;

(iii) Firearms-training instructors conducting training on covered weapons;

(iv) Armorers conducting maintenance, repair, and testing of covered weapons;

(v) Individuals with access to armories and weapons storage lockers containing covered weapons;

(vi) Individuals conducting inventories of enhanced weapons;

(vii) Individuals removing enhanced weapons from the site for repair, training, and escort-duty purposes; and

(viii) Individuals whose duties require access to covered weapons, whether the individuals are employed directly by the licensee or employed by a security contractor who provides security services to the licensee.

(3) The Firearms Background Check Plan must describe how the licensee will accomplish the following objectives:

(i) Completing firearms background checks for all security personnel whose duties require, or will require, access to covered weapons;

(ii) Establishing a process for completing initial, periodic, and break-in-service firearms background checks;

(iii) Defining the training objectives and modules for security personnel who are subject to firearms background checks;

(iv) Completing the initial and periodic training for security personnel whose official duties require access to covered weapons;

(v) Maintaining records of completed firearms background checks, required training, and any supporting documents;

(vi) Maintaining records of a decision to remove security personnel from duties requiring access to covered weapons, due to the identification or occurrence of any Federal or State disqualifying status condition or disqualifying event; and

(vii) Developing and implementing procedures for notifying the NRC of the removal of security personnel from access to covered weapons, due to the identification or occurrence of any Federal or State disqualifying status condition or disqualifying event.

(4)(i) Licensees that have applied to the NRC for stand-alone preemption authority or for combined preemption authority and enhanced weapons authority under § 73.15 must ensure that a satisfactory firearms background check has been completed for all security personnel whose official duties require access to covered weapons.

(ii) Security personal may continue to have access to covered weapons pending the results of the initial firearms background check.

(5) Only licensees that have applied for Section 161A authority under § 73.15

may conduct the firearms background checks required by this section.

(6) The licensee must commence firearms background checks only after receiving notification from the NRC that the agency has accepted for review its application for stand-alone preemption authority or for combined preemption authority and enhanced weapons authority.

(7)(i) Applicants for a license who have also submitted an application for Section 161A authority must only commence firearms background checks after:

(A) The NRC has issued its license; and

(B) The NRC has accepted its application for stand-alone preemption authority or for combined preemption authority and enhanced weapons authority for review.

(ii) Subsequent to April 13, 2023, applicants for a license who have also applied for Section 161A authority and been issued their license must ensure that a satisfactory firearms background check (as defined in §73.2) has been completed for all security personnel who require access to covered weapons, before the licensee's initial receipt of any source material, special nuclear material, or radioactive material specified under the license.

(8) In response to an adverse firearms background check (as defined in §73.2),

(i) The licensee must remove, without delay, from duties requiring access to covered weapons, any security personnel who receive a ''denied'' or ''delayed'' NICS response.

(ii) If the security personnel to be removed is on duty at the time of removal, then the licensee must fill the vacated position within the timeframe specified in its physical security plan.

(9)(i) The licensee must complete a new satisfactory firearms background check for any of its security personnel that has had a break-in-service greater than 1 week.

(ii) The licensee must complete a new satisfactory firearms background check if the security personnel has transferred from a different licensee.

(iii) A break-in-service means the security personnel's cessation of employment with the licensee or its security contractor, notwithstanding that the previous licensee completed a satisfactory firearms background check on the individual within the last 5 years.

(iv) Exceptions: (A) For the purposes of this section, a break-in-service does not include a security personnel's temporary active duty with the U.S. military reserves or National Guard.

(B) The licensee, in lieu of completing a new satisfactory firearms background check, may instead verify, via an industry-wide information-sharing database, that the security personnel has completed a satisfactory firearms background check within the previous 12 months, provided that this previous firearms background check included a duty station location in the State or Territory where the licensee (who would otherwise be accomplishing the firearms background check) is located or the activity is solely occurring.

(10) Changes in the licensee's ownership or its security contractor services are not considered a break-in-service for current security personnel whose duties require access to covered weapons. Licensees are not required to conduct a new firearms background check for these security personnel.

(11) With regard to accomplishing the requirements for other background (e.g., criminal history records) checks or personnel security investigations under the NRC's access authorization or personal security clearance program requirements of this chapter, the licensee may not substitute a satisfactory firearms background check in lieu of completing these other required background checks or security investigations.

(12) If a licensee has completed initial satisfactory firearms background checks pursuant to an NRC order issued before April 13, 2023, then the licensee is not required to conduct a new initial firearms background check for its current security personnel. However, the licensee must conduct initial firearms background checks on new security personnel and periodic and break-in-service firearms background checks on current security personnel in accordance with the provisions of this section.

(13) A licensee who withdraws its application for Section 161A authority or

who has its application disapproved by the NRC, must discontinue conducting firearms background checks.

(14) A licensee whose authority under Section 161A has been rescinded or whose authority has been revoked by the NRC must discontinue conducting firearms background checks.

(c) [Reserved]

(d) *Firearms background check requirements.* A firearms background check for security personnel must include—

(1) A check of the individual's fingerprints against the Federal Bureau of Investigation's (FBI's) fingerprint system; and

(2) A check of the individual's identifying information against the FBI's National Instant Criminal Background Check System (NICS).

(e) *Firearms background check submittals.* (1) Licensees must submit to the NRC, in accordance with § 73.4, for all security personnel requiring a firearms background check under this section—

(i) A set of fingerprint impressions, in accordance with paragraph (k) of this section; and

(ii) A completed NRC Form 754.

(2) In lieu of submitting a copy of each individual completed NRC Form 754 to the NRC, licensees may submit a single document consolidating the NRC Forms 754 data for multiple security personnel.

(3) Licensees submitting to the NRC via an electronic method an individual NRC Form 754 or consolidated data from multiple NRC Forms 754 must ensure that any personally identifiable information contained within these documents is protected in accordance with § 2.390 of this chapter.

(4) Licensees must retain a copy of all NRC Forms 754 submitted to the NRC for one year subsequent to the termination or denial of an individual's access to covered weapons.

(5) Licensees that are Federal agencies with authority to submit fingerprints directly to the FBI may do so provided that they also include the requested information from NRC Form 754. However, such licensees are still required to comply with the other provisions of this section.

(f) *Periodic firearms background checks.* (1) Licensees must complete a satisfactory periodic firearms background check at least once every 5 calendar years for security personnel whose continuing duties require access to covered weapons.

(2) Licensees must complete a periodic firearms background check within the same calendar month as the initial, or most recent, firearms background check with an allowance period to midnight (local time) of the last day of the calendar month of expiration.

(3) The licensee may conduct periodic firearms background checks at an interval of less than once every 5 calendar years, at its discretion.

(4)(i) Licensees may assign security personnel to duties requiring access to covered weapons while the results of the periodic firearms background check are pending.

(ii) Licensees must remove security personnel from duties requiring access to covered weapons if the satisfactory completion of a periodic firearms background check does not occur before the expiration of the allowance period.

(5) Licensees must remove, without delay, from duties requiring access to covered weapons, any security personnel who receive either a ''denied'' or ''delayed'' NICS response during a periodic firearms background check.

(g) *Notification of removal.* (1) Licensees must notify the NRC Headquarters Operations Center by telephone within 72 hours after removing security personnel from duties requiring access to covered weapons due to the identification or occurrence of any Federal or State disqualifying status condition or disqualifying event that would prohibit them from possessing, receiving, or using firearms or ammunition. Licensees must contact the NRC Headquarters Operations Center at the phone numbers specified in Table 1 of appendix A of this part.

(2) The NRC will subsequently inform the FBI of any notifications received under this paragraph.

(h) *Security personnel responsibilities.* Security personnel assigned to duties requiring access to covered weapons must notify the licensee's security management within 72 hours of the identification or occurrence of any Federal or State disqualifying status condition or disqualifying event that

would prohibit the individual from possessing, receiving, or using firearms or ammunition. This requirement is applicable to security personnel directly employed by the licensee or employed by a contractor providing security services to the licensee.

(i) [Reserved]

(j) *Training for security personnel subject to firearms background checks on disqualifying status conditions and disqualifying events.* (1) Licensees must include, within their Firearms Background Check Plan, training modules for security personnel assigned to official duties requiring access to covered weapons that provide training on the following topics:

(i) Federal disqualifying status conditions or disqualifying events specified in 27 CFR 478.32;

(ii) Applicable State disqualifying status conditions or disqualifying events;

(iii) The responsibility of security personnel subject to a firearms background check and assigned to official duties that require access to covered weapons to promptly notify their employing licensee of the occurrence of any disqualifying status condition or disqualifying event; and

(iv) Information for appealing an adverse firearms background check (*i.e.*, a ''denied'' or ''delayed'' NICS response) to the FBI.

(2) Licensees must conduct periodic refresher training on these modules at an annual frequency for security personnel assigned official duties requiring access to covered weapons.

(k) *Procedures for processing fingerprint checks.* (1) Licensees, using an appropriate method listed in §73.4, must manually or electronically submit to the NRC one completed, legible standard fingerprint card (FBI Form FD–258, ORIMDNRCOOOZ) or, where practicable, other electronic fingerprint records for each individual requiring a firearms background check. Information on how to obtain FBI Form FD–258 and the process for manual or electronic submission of fingerprint records to the NRC is on the NRC's public website at: *https://www.nrc.gov/security/chp.html.*

(2) Licensees must indicate on the fingerprint card (or other electronic fingerprint records) that the submittal is part of a firearms background check for personnel whose duties require, or will require, access to covered weapons. Licensees must add the following information to the FBI Form FD–258 fingerprint card or the electronic fingerprint records submitted to the NRC:

(i) For fingerprints submitted to the NRC for the completion of a firearms background check only, the licensee must enter the terms ''MDNRCNICZ'' in the ''ORI'' field and ''Firearms'' in the ''Reasons Fingerprinted'' field of the FBI Form FD–258 or the electronic fingerprint records submitted to the NRC.

(ii) For fingerprints submitted to the NRC for the completion of both an access authorization check or personnel security clearance check and a firearms background check, the licensee must enter the terms ''MDNRC000Z'' in the ''ORI'' field and ''Employment and Firearms'' in the ''Reasons Fingerprinted'' field of the FBI Form FD–258 or the electronic fingerprint records submitted to the NRC.

(3) Licensees must establish procedures that produce high-quality fingerprint images, cards, and records with a minimal rejection rate.

(4) The NRC will review fingerprints for firearms background checks for completeness. Any FBI Form FD–258 or other electronic fingerprint records containing omissions or evident errors will be returned to the licensee for correction. The fee for processing fingerprint checks includes one free resubmission if the initial submission is returned by the FBI because the fingerprint impressions cannot be classified. The one free resubmission must have the FBI Transaction Control Number reflected on the resubmission. If additional submissions are necessary, they will be treated as an initial submittal and require a second payment of the processing fee. The payment of a new processing fee entitles the submitter to an additional free resubmittal, if necessary. Previously rejected submissions may not be included with the third submission because the submittal will be rejected automatically.

(5) The NRC will forward to the submitting licensee all data received from

the FBI as a result of the licensee's application(s) for a firearms background check. This will include the FBI's ''proceed,'' ''delayed,'' or ''denied'' NICS response and the NICS transaction number.

(l) [Reserved]

(m) *Fees.* (1) Fees for the processing of firearms background checks are due upon application. The fee for the processing of a firearms background check consists of a fingerprint fee and a NICS check fee. Licensees must submit payment with the application for the processing of fingerprints, and payment must be made by corporate check, certified check, cashier's check, money order, or electronic payment, made payable to ''U.S. Nuclear Regulatory Commission.'' Combined payment for multiple applications is acceptable. Licensees can find fee information for firearms background checks on the NRC's public website at: *https://www.nrc.gov/security/chp.html.*

(2) The application fee for the processing of fingerprint checks is the sum of the user fee charged by the FBI for each fingerprint card or other fingerprint records submitted by the NRC on behalf of a licensee, and an administrative processing fee assessed by the NRC. The NRC processing fee covers administrative costs associated with NRC handling of licensee fingerprint submissions.

(3) The application fee for the processing of NICS checks is an administrative processing fee assessed by the NRC.

(4) Licensees that are also Federal agencies and submit fingerprints and information contained in the NRC Form 754 directly to the FBI are not assessed an application fee by the NRC.

(n) *Processing of the NICS portion of a firearms background check.* (1) The NRC will forward the information contained in the submitted NRC Form 754 to the FBI for evaluation against the NICS databases. Upon completion of the NICS portion of the firearms background check, the FBI will inform the NRC of the results with one of three responses under 28 CFR part 25; ''proceed,'' ''delayed,'' or ''denied,'' and the associated NICS transaction number (NTN). The NRC will forward these results and the associated NTN to the submitting licensee.

(2) Licensees that are Federal agencies and submit fingerprints and information contained in the NRC Form 754 directly to the FBI for evaluation against the NICS databases will receive one of three responses under 28 CFR part 25; ''proceed,'' ''delayed,'' or ''denied,'' and the associated NTN.

(3) The submitting licensee must provide these results to the individual who completed the NRC Form 754.

(o) [Reserved]

(p) *Appeals and resolution of adverse firearms background checks.* (1) Licensees may not assign security personnel who have received a ''denied'' or a ''delayed'' NICS response to any official duties requiring access to covered weapons—

(i) During the pendency of an appeal to the FBI of a ''denied'' NICS response; or

(ii) During the pendency of providing to the FBI any necessary additional information to resolve a ''delayed'' NICS response.

(2) Licensees must provide the NICS Transaction Number (NTN) or NTNs associated with the adverse firearms background check to the affected individual. It is the affected individual's responsibility to initiate an appeal or resolution of a ''delayed'' or ''denied'' NICS response.

(3) Licensees may assign security personnel to official duties requiring access to covered weapons subsequent to the individual's satisfactorily resolving a ''denied'' or ''delayed'' NICS response.

(q) *Protection of information.* (1) Each licensee that obtains a firearms background check and NRC Form 754 information on individuals under this section shall establish and maintain a system of files and procedures to protect these records and any enclosed personally identifiable information (PII) from unauthorized disclosure.

(2) The licensee may not disclose these records or PII to persons other than the subject individual, his/her representative, or to those with a need to have access to the information in performing assigned duties in the process of granting access to covered weapons. No individual authorized to have access

to this information may disseminate the information to any other individual who does not have a need to know.

(3) The record or PII may be disclosed to an appropriate Federal or State agency in the performance of its official duties, in the course of an administrative or judicial proceeding, or in response to a Congressional inquiry.

(4) The licensee must make firearms background check records and NRC Forms 754 obtained under this section available for examination by an authorized representative of the NRC to determine compliance with applicable regulations and laws.

(5) The record obtained on an individual from a firearms background check may be transferred to another licensee—

(i) Upon an individual's written request to transfer the individual's record to the licensee identified in the written request; and

(ii) Upon verification from the gaining licensee of the individual's name, date of birth, social security number, and sex.

(r) *Withdrawal of orders.* In accordance with the provisions of §73.15(s), orders issued under Section 161A (42 U.S.C. 2201a) prior to April 13, 2023 are withdrawn. Accordingly, the requirements of those orders are superseded in their entirety by the requirements of §§73.15 and 73.17.

Subpart C—General Performance Objective for Protection of Strategic Special Nuclear Material

§73.20 General performance objective and requirements.

(a) In addition to any other requirements of this part, each licensee who is authorized to operate a fuel reprocessing plant pursuant to part 50 of this chapter; possesses or uses formula quantities of strategic special nuclear material at any site or contiguous sites subject to control by the licensee; is authorized to transport or deliver to a carrier for transportation pursuant to part 70 of this chapter formula quantities of strategic special nuclear material; takes delivery of formula quantities of strategic special nuclear material free on board (f.o.b.) the point at which it is delivered to a carrier for transportation; or imports or exports formula quantities of strategic special nuclear material, shall establish and maintain or make arrangements for a physical protection system 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 threats of theft or diversion of strategic special nuclear material and radiological sabotage as stated in §73.1(a).

(b) To achieve the general performance objective of paragraph (a) of this section a licensee shall establish and maintain, or arrange for, a physical protection system that:

(1) Provides the performance capabilities described in §73.25 for in-transit protection or in §73.45 for fixed site protection unless otherwise authorized by the Commission;

(2) Is designed with sufficient redundancy and diversity to ensure maintenance of the capabilities described in §§73.25 and 73.45;

(3) Includes a safeguards contingency capability that can meet the criteria in appendix C to this part ''Licensee Safeguards Contingency Plans;'' and

(4) Includes a testing and maintenance program to assure control over all activities and devices affecting the effectiveness, reliability, and availability of the physical protection system, including a demonstration that any defects of such activities and devices will be promptly detected and corrected for the total period of time they are required as a part of the physical protection system.

(c) Each licensee subject to the requirements of paragraphs (a) and (b) of this section shall establish, maintain, and follow NRC-approved safeguards physical protection and safeguards contingency plans that describe how the licensee will comply with the requirements of paragraphs (a) and (b) of this section.

[44 FR 68188, Nov. 28, 1979, as amended at 57 FR 33430, July 29, 1992]

Subpart D—Protection of Safeguards Information

SOURCE: 88 FR 15890, Mar. 14, 2023, unless otherwise noted.

§ 73.21 Protection of Safeguards Information: Performance requirements.

(a) *General performance requirement.* (1) Each licensee, certificate holder, applicant, or other person who produces, receives, or acquires Safeguards Information (including Safeguards Information with the designation or marking: Safeguards Information—Modified Handling) shall ensure that it is protected against unauthorized disclosure. To meet this general performance requirement, such licensees, certificate holders, applicants, or other persons subject to this section shall:

(i) Establish, implement, and maintain an information protection system that includes the applicable measures for Safeguards Information specified in § 73.22 related to: Power reactors; a formula quantity of strategic special nuclear material; transportation of or delivery to a carrier for transportation of a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel; uranium hexafluoride production or conversion facilities; fuel fabrication facilities; uranium enrichment facilities; independent spent fuel storage installations; and geologic repository operations areas.

(ii) Establish, implement, and maintain an information protection system that includes the applicable measures for Safeguards Information specified in § 73.23 related to: Research and test reactors that possess special nuclear material of moderate strategic significance or special nuclear material of low strategic significance.

(iii) Protect the information in accordance with the requirements of § 73.22 if the Safeguards Information is not described in paragraphs (a)(1)(i) and (a)(1)(ii) of this section.

(2) Information protection procedures employed by Federal, State, Tribal, and local law enforcement agencies are presumed to meet the general performance requirement in paragraph (a)(1) of this section.

(b) *Commission authority.* (1) Pursuant to Section 147 of the Atomic Energy Act of 1954, as amended, the Commission may impose, by order or regulation, Safeguards Information protection requirements different from or in addition to those specified in this Part on any person who produces, receives, or acquires Safeguards Information.

(2) The Commission may require, by regulation or order, that information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, related to facilities or materials not specifically described in §§ 73.21, 73.22 or 73.23 be protected under this part.

[73 FR 63574, Oct. 24, 2008, as amended at 77 FR 34205, June 11, 2012; 79 FR 58671, Sept. 30, 2014]

§ 73.22 Protection of Safeguards Information: Specific requirements.

This section contains specific requirements for the protection of Safeguards Information in the hands of any person subject to the requirements of § 73.21(a)(1)(i) and related to power reactors; a formula quantity of strategic special nuclear material; transportation of or delivery to a carrier for transportation of a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel; uranium hexafluoride production or conversion facilities, fuel fabrication facilities, and uranium enrichment facilities; independent spent fuel storage installations; geologic repository operations areas and Safeguards Information in the hands of any person subject to the requirements of § 73.21(a)(1)(iii).

(a) *Information to be protected.* The types of information and documents that must be protected as Safeguards Information include non-public security-related requirements such as:

(1) *Physical protection.* Information not classified as Restricted Data or National Security Information related to physical protection, including:

(i) The composite physical security plan for the facility or site;

(ii) Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical security system not easily discernible by members of the public;

(iii) Alarm system layouts showing the location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources for security equipment, and duress alarms not easily discernible by members of the public;

(iv) Physical security orders and procedures issued by the licensee for members of the security organization detailing duress codes, patrol routes and schedules, or responses to security contingency events;

(v) Site-specific design features of plant security communications systems;

(vi) Lock combinations, mechanical key design, or passwords integral to the physical security system;

(vii) Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified in the documents or other matter as vital for purposes of physical protection, as contained in security plans, contingency measures, or plant specific safeguards analyses;

(viii) The composite safeguards contingency plan/measures for the facility or site;

(ix) The composite facility guard qualification and training plan/measures disclosing features of the physical security system or response procedures;

(x) Information relating to on-site or off-site response forces, including size, armament of response forces, and arrival times of such forces committed to respond to security contingency events;

(xi) The adversary characteristics document and related information, including implementing guidance associated with the Design Basis Threat in §73.1(a)(1) or (a)(2); and

(xii) Engineering and safety analyses, security-related procedures or scenarios, and other information revealing site-specific details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.

(2) *Physical protection in transit.* Information not classified as Restricted Data or National Security Information related to the transportation of, or delivery to a carrier for transportation of a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel, including:

(i) The composite physical security plan for transportation;

(ii) Schedules and itineraries for specific shipments of source material, byproduct material, high-level nuclear waste, or irradiated reactor fuel. Schedules for shipments of source material, byproduct material, high-level nuclear waste, or irradiated reactor fuel are no longer controlled as Safeguards Information 10 days after the last shipment of a current series;

(iii) Vehicle immobilization features, intrusion alarm devices, and communications systems;

(iv) Arrangements with and capabilities of local police response forces, and locations of safe havens identified along the transportation route;

(v) Limitations of communications during transport;

(vi) Procedures for response to security contingency events;

(vii) Information concerning the tactics and capabilities required to defend against attempted sabotage, or theft and diversion of formula quantities of special nuclear material, irradiated reactor fuel, or related information; and

(viii) Engineering or safety analyses, security-related procedures or scenarios and other information related to the protection of the transported material if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.

(3) *Inspections, audits and evaluations.* Information not classified as National Security Information or Restricted

Data pertaining to safeguards and security inspections and reports, including:

(i) Portions of inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. Disclosure of corrected defects, weaknesses, or vulnerabilities is subject to an assessment taking into account such factors as trending analyses and the impacts of disclosure on licensees having similar physical security systems; and

(ii) Reports of investigations containing general information may be released after corrective actions have been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).

(4) *Correspondence.* Portions of correspondence insofar as they contain Safeguards Information as set forth in paragraphs (a)(1) through (a)(3) of this section.

(5) Other information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, that the Commission determines by order or regulation could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material or a facility.

(b) *Conditions for access.* (1) Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established ''need to know'' for the information and has undergone a Federal Bureau of Investigation (FBI) criminal history records check using the procedures set forth in § 73.57.

(2) In addition, a person to be granted access to Safeguards Information must be trustworthy and reliable, based on a background check or other means approved by the Commission.

(3) The categories of individuals specified in 10 CFR 73.59 are exempt from the criminal history records check and background check requirements in paragraphs (b)(1) and (b)(2) of this section by virtue of their occupational status.

(4) For persons participating in an NRC adjudicatory proceeding, the ''need to know'' determination shall be made by the originator of the Safeguards Information upon receipt of a request for access to the Safeguards Information. Where the information is in the possession of the originator and the NRC staff, whether in its original form or incorporated into another document or other matter by the recipient, the NRC staff shall make the determination. In the event of a dispute regarding the ''need to know'' determination, the presiding officer of the proceeding shall determine whether the ''need to know'' findings in § 73.2 can be made.

(5) Except as the Commission may otherwise authorize, no person may disclose Safeguards Information to any other person except as set forth in this section.

(c) *Protection while in use or storage.* (1) While in use, matter containing Safeguards Information must be under the control of an individual authorized access to Safeguards Information. This requirement is satisfied if the Safeguards Information is attended by such an individual even though the information is in fact not constantly being used. Safeguards Information within alarm stations, or rooms continuously occupied by authorized individuals need not be stored in a locked security storage container.

(2) While unattended, Safeguards Information must be stored in a locked security storage container. The container shall not identify the contents of the matter contained and must preclude access by individuals not authorized access in accordance with the provisions of this section. Knowledge of lock combinations protecting Safeguards Information must be limited to a minimum number of personnel for operating purposes who have a ''need to know'' and are otherwise authorized access to Safeguards Information in accordance with the provisions of this Part. Access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to Safeguards Information.

(d) *Preparation and marking of documents or other matter.* (1) Each document or other matter that contains Safeguards Information as described in § 73.21(a)(1)(i) and this section must be marked to indicate the presence of such information in a conspicuous manner on the top and bottom of each page. The first page of the document or other matter must also contain:

(i) The name, title, and organization of the individual authorized to make a Safeguards Information determination, and who has determined that the document or other matter contains Safeguards Information;

(ii) The date the determination was made; and

(iii) An indication that unauthorized disclosure will be subject to civil and criminal sanctions.

(2) In addition to the markings at the top and bottom of each page, any transmittal letters or memoranda to or from the NRC which do not in themselves contain Safeguards Information shall be marked to indicate that attachments or enclosures contain Safeguards Information but that the transmittal document or other matter does not (*i.e.*, ''When separated from Safeguards Information enclosure(s), this document is decontrolled provided the transmittal document does not otherwise warrant protection from unauthorized disclosure'').

(3) Any transmittal document or other matter forwarding Safeguards Information must alert the recipient that protected information is enclosed. Certification that a document or other matter contains Safeguards Information must include the name and title of the certifying official and date designated. Portion marking is required only for correspondence to and from the NRC (*i.e.*, cover letters, but not attachments) that contains Safeguards Information. The portion marking must be sufficient to allow the recipient to identify and distinguish those sections of the transmittal document or other information containing the Safeguards Information from non-Safeguards Information.

(4) Marking of documents or other matter containing or transmitting Safeguards Information shall, at a minimum include the words ''Safeguards Information'' to ensure identification of protected information for the protection of facilities and material covered by § 73.22.

(e) *Reproduction of matter containing Safeguards Information.* Safeguards Information may be reproduced to the minimum extent necessary consistent with need without permission of the originator. Equipment used to reproduce Safeguards Information must be evaluated to ensure that unauthorized individuals cannot access Safeguards Information (e.g., unauthorized individuals cannot access Safeguards Information by gaining access to retained memory or network connectivity).

(f) *External transmission of documents and material.* (1) Documents or other matter containing Safeguards Information, when transmitted outside an authorized place of use or storage, must be packaged in two sealed envelopes or wrappers to preclude disclosure of the presence of protected information. The inner envelope or wrapper must contain the name and address of the intended recipient and be marked on both sides, top and bottom, with the words ''Safeguards Information.'' The outer envelope or wrapper must be opaque, addressed to the intended recipient, must contain the address of the sender, and may not bear any markings or indication that the document or other matter contains Safeguards Information.

(2) Safeguards Information may be transported by any commercial delivery company that provides service with computer tracking features, U.S. first class, registered, express, or certified mail, or by any individual authorized access pursuant to these requirements.

(3) Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted outside an authorized place of use or storage only by NRC approved secure electronic devices, such as facsimiles or telephone devices, provided that transmitters and receivers implement processes that will provide high assurance that Safeguards Information is protected before and after the transmission or electronic mail through the internet, provided that the information is encrypted by a method (Federal Information Processing Standard [FIPS]

140–2 or later) approved by the appropriate NRC Office; the information is produced by a self contained secure automatic data process system; and transmitters and receivers implement the information handling processes that will provide high assurance that Safeguards Information is protected before and after transmission. Physical security events required to be reported pursuant to § 73.1200 are considered to be extraordinary conditions. Cyber security event notifications required to be reported pursuant to § 73.77 are considered to be extraordinary conditions.

(g) *Processing of Safeguards Information on electronic systems.* (1) Safeguards Information may be stored, processed or produced on a stand-alone computer (or computer system) for processing of Safeguards Information. ''Stand-alone'' means a computer or computer system to which access is limited to individuals authorized access to Safeguards Information. A stand-alone computer or computer system shall not be physically or in any other way connected to a network accessible by users who are not authorized access to Safeguards Information.

(2) Each computer not located within an approved and lockable security storage container that is used to process Safeguards Information must have a removable storage medium with a bootable operating system. The bootable operating system must be used to load and initialize the computer. The removable storage medium must also contain the software application programs. Data may be saved on either the removable storage medium that is used to boot the operating system, or on a different removable storage medium. The removable storage medium must be secured in a locked security storage container when not in use.

(3) A mobile device (such as a laptop computer) may also be used for the processing of Safeguards Information provided the device is secured in a locked security storage container when not in use. Other systems may be used if approved for security by the appropriate NRC office.

(4) Any electronic system that has been used for storage, processing or production of Safeguards Information must be free of recoverable Safeguards Information prior to being returned to nonexclusive use.

(h) *Removal from Safeguards Information category.* Documents or other matter originally containing Safeguards Information must be removed from the Safeguards Information category at such time as the information no longer meets the criteria contained in this part. Care must be exercised to ensure that any document or other matter decontrolled not disclose Safeguards Information in some other form or be combined with other unprotected information to disclose Safeguards Information. The authority to determine that a document or other matter may be decontrolled will only be exercised by the NRC, with NRC approval, or in consultation with the individual or organization that made the original determination.

(i) *Destruction of matter containing Safeguards Information.* Documents or other matter containing Safeguards Information shall be destroyed when no longer needed. The information can be destroyed by burning, shredding or any other method that precludes reconstruction by means available to the public at large. Piece sizes no wider than one quarter inch composed of several pages or documents and thoroughly mixed are considered completely destroyed.

[73 FR 63574, Oct. 24, 2008, as amended at 80 FR 67275, Nov. 2, 2015; 88 FR 15890, Mar. 14, 2023]

§ 73.23 Protection of Safeguards Information—Modified Handling: Specific requirements.

This section contains specific requirements for the protection of Safeguards Information in the hands of any person subject to the requirements of § 73.21(a)(1)(ii) and research and test reactors that possess special nuclear material of moderate strategic significance or special nuclear material of low strategic significance. The requirements of this section distinguish Safeguards Information requiring modified handling requirements (SGI–M) from the specific Safeguards Information handling requirements applicable to facilities and materials needing a higher

level of protection, as set forth in § 73.22.

(a) *Information to be protected.* The types of information and documents that must be protected as Safeguards Information—Modified Handling include non-public security-related requirements such as protective measures, interim compensatory measures, additional security measures, and the following, as applicable:

(1) *Physical protection.* Information not classified as Restricted Data or National Security Information related to physical protection, including:

(i) The composite physical security plan for the facility or site;

(ii) Site specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical security system not easily discernible by members of the public;

(iii) Alarm system layouts showing the location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources for security equipment, and duress alarms not easily discernible by members of the public;

(iv) Physical security orders and procedures issued by the licensee for members of the security organization detailing duress codes, patrol routes and schedules, or responses to security contingency events;

(v) Site specific design features of plant security communications systems;

(vi) Lock combinations, mechanical key design, or passwords integral to the physical security system;

(vii) The composite facility guard qualification and training plan/measures disclosing features of the physical security system or response procedures;

(viii) Descriptions of security activities which disclose features of the physical security system or response measures;

(ix) Information relating to onsite or offsite response forces, including size, armament of the response forces, and arrival times of such forces committed to respond to security contingency events; and

(x) Engineering and safety analyses, security-related procedures or scenarios, and other information revealing site-specific details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.

(2) *Physical protection in transit.* Information not classified as Restricted Data or National Security Information related to the physical protection of shipments of special nuclear material in less than a formula quantity (except for those materials covered under § 73.22), including:

(i) Information regarding transportation security measures, including physical security plans and procedures, immobilization devices, and escort requirements, more detailed than NRC regulations;

(ii) Scheduling and itinerary information for shipments (scheduling and itinerary information for shipments that are inherently self-disclosing, such as a shipment that created extensive news coverage or an announcement by a public official confirming receipt, may be decontrolled after shipment departure). Scheduling and itinerary information for shipments that are not inherently self-disclosing may be decontrolled 2 days after the shipment is completed. Scheduling and itinerary information used for the purpose of preplanning, coordination, and advance notification may be shared with others on a ''need to know'' basis and need not be designated as Safeguards Information-Modified Handling);

(iii) Arrangements with and capabilities of local police response forces, and locations of safe havens identified along the transportation route;

(iv) Details of alarm and communication systems, communication procedures, and duress codes;

(v) Procedures for response to security contingency events; and

(vi) Engineering or safety analyses, security-related procedures or scenarios and other information related to the protection of the transported material if the unauthorized disclosure of

such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material.

(3) *Inspections, audits and evaluations.* Information not classified as National Security Information or Restricted Data pertaining to safeguards and security inspections and reports, including:

(i) Portions of inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. Disclosure of corrected defects, weaknesses, or vulnerabilities is subject to an assessment taking into account such factors as trending analyses and the impacts of disclosure on licensees having similar physical security systems; and

(ii) Reports of investigations containing general information may be released after the corrective actions have been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).

(4) *Correspondence.* Portions of correspondence insofar as they contain Safeguards Information designated as Safeguards Information-Modified Handling, as set forth in paragraphs (a)(1) through (a)(3) of this section.

(5) Other information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, that the Commission determines by order or regulation could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, byproduct, or special nuclear material or a facility.

(b) *Conditions for access.* (1) Except as the Commission may otherwise authorize, no person may have access to Safeguards Information designated as Safeguards Information-Modified Handling unless the person has an established ''need to know'' for the information and has undergone a Federal Bureau of Investigation criminal history records check using the procedures set forth in § 73.57.

(2) In addition, a person to be granted access to Safeguards Information must be trustworthy and reliable, based on a background check or other means approved by the Commission.

(3) The categories of individuals specified in 10 CFR 73.59 are exempt from the criminal history records check and background check requirements in paragraphs (b)(1) and (b)(2) of this section by virtue of their occupational status:

(4) For persons participating in an NRC adjudicatory proceeding, the ''need to know'' determination shall be made by the originator of the Safeguards Information designated as Safeguards Information-Modified Handling upon receipt of a request for access to the Safeguards Information designated as Safeguards Information-Modified Handling. Where the information is in the possession of the originator and the NRC staff, whether in its original form or incorporated into another document or other matter by the recipient, the NRC staff shall make the determination. In the event of a dispute regarding the ''need to know'' determination, the presiding officer of the proceeding shall determine whether the ''need to know'' findings in § 73.2 can be made.

(5) Except as the Commission may otherwise authorize, no person may disclose Safeguards Information designated as Safeguards Information-Modified Handling to any other person except as set forth in this section.

(c) *Protection while in use or storage.* (1) While in use, matter containing Safeguards Information designated as Safeguards Information-Modified Handling must be under the control of an individual authorized access to such information. This requirement is satisfied if the Safeguards Information designated as Safeguards Information-Modified Handling is attended by such an individual even though the information is in fact not constantly being used. Safeguards Information designated as Safeguards Information-Modified Handling within alarm stations, or rooms continuously occupied

by authorized individuals, need not be locked in a file drawer or cabinet.

(2) While unattended, Safeguards Information designated as Safeguards Information-Modified Handling must be stored in a locked file drawer or cabinet. The container shall not identify the contents of the matter contained and must preclude access by individuals not authorized access in accordance with the provisions of this section. Knowledge of lock combinations or access to keys protecting Safeguards Information designated as Safeguards Information-Modified Handling must be limited to a minimum number of personnel for operating purposes who have a ''need to know'' and are otherwise authorized access to Safeguards Information in accordance with the provisions of this Part. Access to lock combinations must be strictly controlled so as to prevent disclosure to an individual not authorized access to Safeguards Information designated as Safeguards Information-Modified Handling.

(d) *Preparation and marking of documents or other matter.* (1) Each document or other matter that contains Safeguards Information designated as Safeguards Information-Modified Handling as described in § 73.23(a) and in this section must be marked to indicate the presence of Safeguards Information with modified handling requirements in a conspicuous manner on the top and bottom of each page. The first page of the document or other matter must also contain:

(i) The name, title, and organization of the individual authorized to make a ''Safeguards Information designated as Safeguards Information-Modified Handling'' determination, and who has determined that the document or other matter contains Safeguards Information designated as Safeguards Information-Modified Handling;

(ii) The date the determination was made; and

(iii) An indication that unauthorized disclosure will be subject to civil and criminal sanctions.

(2) In addition to the markings at the top and bottom of each page, any transmittal letters or memoranda to or from the NRC which do not in themselves contain Safeguards Information designated as Safeguards Information-Modified Handling shall be marked to indicate that attachments or enclosures contain Safeguards Information designated as Safeguards Information-Modified Handling but that the transmittal document does not (*i.e.*, ''When separated from Safeguards Information designated as Safeguards Information-Modified Handling enclosure(s), this document is decontrolled provided the transmittal document does not otherwise warrant protection from unauthorized disclosure'').

(3) Any transmittal document or other matter forwarding Safeguards Information designated as Safeguards Information-Modified Handling must alert the recipient that protected information is enclosed. Certification that a document or other matter contains Safeguards Information designated as Safeguards Information-Modified Handling must include the name and title of the certifying official and date designated. Portion marking is required only for correspondence to and from the NRC (*i.e.*, cover letters, but not attachments) that contains Safeguards Information designated as Safeguards Information-Modified Handling. The portion marking must be sufficient to allow the recipient to identify and distinguish those sections of the transmittal document or other information containing the Safeguards Information from non-Safeguards Information.

(4) Marking of documents or other matter containing or transmitting Safeguards Information with modified handling requirements shall, at a minimum include the words ''Safeguards Information-Modified Handling'' to ensure identification of protected information for the protection of facilities and material covered by § 73.23.

(e) *Reproduction of matter containing Safeguards Information designated as Safeguards Information-Modified Handling.* Safeguards Information designated as Safeguards Information-Modified Handling may be reproduced to the minimum extent necessary, consistent with need, without permission of the originator. Equipment used to reproduce Safeguards Information designated as Safeguards Information-Modified Handling must be evaluated

to ensure that unauthorized individuals cannot access the information (e.g. , unauthorized individuals cannot access Safeguards Information by gaining access to retained memory or network connectivity).

(f) *External transmission of documents and material.* (1) Documents or other matter containing Safeguards Information designated as Safeguards Information-Modified Handling, when transmitted outside an authorized place of use or storage, must be packaged in two sealed envelopes or wrappers to preclude disclosure of the presence of protected information. The inner envelope or wrapper must contain the name and address of the intended recipient and be marked on both sides, top and bottom, with the words ''Safeguards Information-Modified Handling.'' The outer envelope or wrapper must be opaque, addressed to the intended recipient, must contain the address of the sender, and may not bear any markings or indication that the document contains Safeguards Information designated as Safeguards Information-Modified Handling.

(2) Safeguards Information designated Safeguards Information-Modified Handling may be transported by any commercial delivery company that provides service with computer tracking features, U.S. first class, registered, express, or certified mail, or by any individual authorized access pursuant to these requirements.

(3) Except under emergency or extraordinary conditions, Safeguards Information designated as Safeguards Information-Modified Handling must be transmitted electronically only by protected telecommunications circuits (including facsimile) or encryption by a method (Federal Information Processing Standard [FIPS] 140–2 or later) approved by the appropriate NRC office. For the purpose of this section, emergency or extraordinary conditions are defined as any circumstances that require immediate communications in order to report, summon assistance for, or respond to a security contingency event or an event that has potential security significance. Physical security events required to be reported pursuant to §§ 73.1200 and 73.1205 are considered to be extraordinary conditions.

(g) *Processing of Safeguards Information-Modified Handling on electronic systems.* (1) Safeguards Information designated for modified handling may be stored, processed or produced on a computer or computer system, provided that the system is assigned to the licensee's or contractor's facility. Safeguards Information designated as Safeguards Information-Modified Handling files must be protected, either by a password or encryption, to prevent unauthorized individuals from gaining access. Word processors such as typewriters are not subject to these requirements as long as they do not transmit information off-site.

NOTE: If Safeguards Information designated as Safeguards Information-Modified Handling is produced on a typewriter, the ribbon must be properly marked and be removed and stored in the same manner as other Safeguards Information designated as Safeguards Information-Modified Handling.

(2) Safeguards Information designated as Safeguards Information-Modified Handling files may be transmitted over a network if the file is encrypted. In such cases, the licensee will select a commercially available encryption system that the National Institute of Standards and Technology (NIST) has validated as conforming to Federal Information Processing Standards (FIPS) 140–2 or later. Safeguards Information designated as Safeguards Information-Modified Handling files shall be properly labeled to indicate the presence of Safeguards Information with modified handling requirements and saved to removable matter and stored in a locked file drawer or cabinet.

(3) A mobile device (such as a laptop computer) may also be used for the processing of Safeguards Information designated as Safeguards Information-Modified Handling provided the device is secured in an appropriate locked storage container when not in use. Other systems may be used if approved for security by the appropriate NRC office.

(4) Any electronic system that has been used for storage, processing or production of Safeguards Information must be free of recoverable Safeguards Information designated as Safeguards

Information-Modified Handling prior to being returned to nonexclusive use.

(h) *Removal from Safeguards Information-Modified Handling category.* Documents or other matter originally containing Safeguards Information designated as Safeguards Information-Modified Handling must be removed from the Safeguards Information category at such time as the information no longer meets the criteria contained in this Part. Care must be exercised to ensure that any document or other matter decontrolled shall not disclose Safeguards Information in some other form or be combined with other unprotected information to disclose Safeguards Information. The authority to determine that a document or other matter may be decontrolled will only be exercised by the NRC, with NRC approval, or in consultation with the individual or organization that made the original determination.

(i) *Destruction of matter containing Safeguards Information designated as Safeguards Information-Modified Handling.* Documents or other matter containing Safeguards Information shall be destroyed when no longer needed. The information can be destroyed by burning, shredding, or any other method that precludes reconstruction by means available to the public at large. Piece sizes no wider than one quarter inch composed of several pages or documents and thoroughly mixed are considered completely destroyed.

[73 FR 63577, Oct. 24, 2008, as amended at 88 FR 15890, Mar. 14, 2023]

Subpart E—Physical Protection Requirements of Special Nuclear Material and Spent Nuclear Fuel in Transit

SOURCE: 88 FR 15890, Apr. 13, 2023, unless otherwise noted.

§ 73.24 Prohibitions.

(a) Except as specifically approved by the Nuclear Regulatory Commission, no shipment of special nuclear material shall be made in passenger aircraft in excess of (1) 20 grams or 20 curies, whichever is less, of plutonium or uranium-233, or (2) 350 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope).

(b) Unless otherwise approved by the Nuclear Regulatory Commission, no licensee may make shipments of special nuclear material in which individual shipments are less than a formula quantity, but the total quantity in shipments in transit at the same time could equal or exceed a formula quantity, unless either of the following conditions are met:

(1) The licensee shall confirm and log the arrival at the final destination of each individual shipment and retain the log for three years from the date of the last entry in the log. The licensee shall also schedule shipments to ensure that the total quantity for two or more shipments in transit at the same time does not equal or exceed the formula quantity, or

(2) Physical protection in accordance with the requirements of §§ 73.20, 73.25, and 73.26 is provided by the licensee for such shipments as appropriate so that the total quantity of special nuclear material in the remaining shipments not so protected, and in transit at the same time, does not equal or exceed a formula quantity.

[44 FR 68188, Nov. 28, 1979, as amended at 53 FR 19257, May 27, 1988]

§ 73.25 Performance capabilities for physical protection of strategic special nuclear material in transit.

(a) To meet the general performance objective and requirements of § 73.20 an in-transit physical protection system shall include the performance capabilities described in paragraphs (b) through (d) of this section unless otherwise authorized by the Commission.

(b) Restrict access to and activity in the vicinity of transports and strategic special nuclear material. To achieve this capability the physical protection system shall:

(1) Minimize the vulnerability of the strategic special nuclear material by using the following subfunctions and procedures:

(i) Preplanning itineraries for the movement of strategic special nuclear material;

(ii) Periodically updating knowledge of route conditions for the movement of strategic special nuclear material;

(iii) Maintaining knowledge of the status and position of the strategic special nuclear material en route; and

(iv) Determining and communicating alternative itineraries en route as conditions warrant.

(2) Detect and delay any unauthorized attempt to gain access or introduce unauthorized materials by stealth or force into the vicinity of transports and strategic special nuclear material using the following subsystems and subfunctions:

(i) Controlled access areas to isolate strategic special nuclear material and transports to assure that unauthorized persons shall not have direct access to, and unauthorized materials shall not be introduced into the vicinity of, the transports and strategic special nuclear material, and

(ii) Access detection subsystems and procedures to detect, assess and communicate any unauthorized penetration (or such attempts) of a controlled access area by persons, vehicles or materials so that the response will satisfy the general performance objective and requirements of § 73.20(a).

(3) Detect attempts to gain unauthorized access or introduce unauthorized materials into the vicinity of transports by deceit using the following subsystems and subfunctions:

(i) Access authorization controls and procedures to provide current authorization schedules and access criteria for persons, materials and vehicles; and

(ii) Access controls and procedures to verify the identity of persons, materials and vehicles, to assess such identity against current authorization schedules and access criteria before permitting access, and to initiate response measures to deny unauthorized entries.

(c) Prevent or delay unauthorized entry or introduction of unauthorized materials into, and unauthorized removal of, strategic special nuclear material from transports. To achieve this capability the physical protection system shall:

(1) Detect attempts to gain unauthorized entry or introduce unauthorized materials into transports by deceit using the following subsystems and subfunctions:

(i) Access authorization controls and procedures to provide current authorization schedules and entry criteria for access into transports for both persons and materials; and

(ii) Entry controls and procedures to verify the identity of persons and materials and to permit transport entry only to those persons and materials specified by the current authorization schedules and entry criteria.

(2) Detect attempts to gain unauthorized entry or introduce unauthorized material into transports by stealth or force using the following subsystems and subfunctions:

(i) Transport features to delay access to strategic special nuclear material sufficient to permit the detection and response systems to function so as to satisfy the general performance objective and requirements of § 73.20(a);

(ii) Inspection and detection subsystems and procedures to detect unauthorized tampering with transports and cargo containers; and

(iii) Surveillance subsystems and procedures to detect, assess and communicate any unauthorized presence of persons or materials and any unauthorized attempt to penetrate the transport so that the response will satisfy the general performance objective and requirements of § 73.20(a).

(3) Prevent unauthorized removal of strategic special nuclear material from transports by deceit using the following subsystems and subfunctions:

(i) Authorization controls and procedures to provide current schedules for authorized removal of strategic special nuclear material which specify the persons authorized to remove and receive the material, the authorized times for such removal and receipt and authorized places for such removal and receipt.

(ii) Removal controls and procedures to establish activities for transferring cargo in emergency situations; and

(iii) Removal controls and procedures to permit removal of strategic special nuclear material only after verification of the identity of persons removing or receiving the strategic special nuclear material, and after verification of the identity and integrity of the strategic special nuclear

material being removed from transports.

(4) Detect attempts to remove strategic special nuclear material from transports by stealth or force using the following subsystems and subfunctions:

(i) Transport features to delay unauthorized strategic special nuclear material removal attempts sufficient to assist detection and permit a response to satisfy the general performance objective and requirements of §73.20(a); and

(ii) Detection subsystems and procedures to detect, assess and communicate any attempts at unauthorized removal of strategic special nuclear material so that response to the attempt can be such as to satisfy the general performance objective and requirements of §73.20(a).

(d) Respond to safeguards contingencies and emergencies to assure that the two capabilities in paragraphs (b) and (c) of this section are achieved, and to engage and impede adversary forces until local law enforcement forces arrive. To achieve this capability, the physical protection system shall:

(1) Respond rapidly and effectively to safeguards contingencies and emergencies using the following subsystems and subfunctions:

(i) A security organization composed of trained and qualifed personnel, including armed escorts, one of whom is designated as escort commander, with procedures for command and control, to execute response functions.

(ii) Assessment procedures to assess the nature and extent of security related incidents.

(iii) A predetermined plan to respond to safeguards contingency events.

(iv) Equipment and procedures to enable responses to security related incidents sufficiently rapid and effective to achieve the predetermined objective of each action.

(v) Equipment, vehicle design features, and procedures to protect security organization personnel, including those at the movement control center, in their performance of assessment and response related functions.

(2) Transmit detection, assessment and other response related information using the following subsystems and subfunctions:

(i) Communications equipment and procedures to rapidly and accurately transmit security information among armed escorts.

(ii) Equipment and procedures for two-way communications between the escort commander and the movement control center to rapidly and accurately transmit assessment information and requests for assistance by local law enforcement forces, and to coordinate such assistance.

(iii) Communications equipment and procedures for the armed escorts and the movement control center personnel to notify local law enforcement forces of the need for assistance.

(3) Establish liaisons with local law enforcement authorities to arrange for assistance en route.

(4) Assure that a single adversary action cannot destroy the capability of armed escorts to notify the local law enforcement forces of the need for assistance.

[44 FR 68188, Nov. 28, 1979]

§73.26 Transportation physical protection systems, subsystems, components, and procedures.

(a) A transportation physical protection system established pursuant to the general performance objectives and requirements of §73.20 and performance capability requirements of §73.25 shall include, but are not necessarily limited to, the measures specified in paragraphs (b) through (l) of this section. The Commission may require, depending on the individual transportation conditions or circumstances, alternate or additional measures deemed necessary to meet the general performance objectives and requirements of §73.20. The Commission also may authorize protection measures other than those required by this section if, in its opinion, the overall level of performance meets the general performance objectives and requirements of §73.20 and the performance capability requirements of §73.25.

(b) *Planning and scheduling.* (1) Shipments shall be scheduled to avoid regular patterns and preplanned to avoid areas of natural disaster or civil disorders, such as strikes or riots. Such shipments shall be planned in order to avoid storage times in excess of 24

hours and to assure that deliveries occur at a time when the receiver at the final delivery point is present to accept the shipment.

(2) Arrangements shall be made with law enforcement authorities along the route of shipments for their response to an emergency or a call for assistance.

(3) Security arrangements for each shipment shall be approved by the Nuclear Regulatory Commission prior to the time for the seven-day notice required by § 73.72. Information to be supplied to the Commission in addition to the general security plan information is as follows:

(i) Shipper, consignee, carriers, transfer points, modes of shipment,

(ii) Point where escorts will relinquish responsibility or will accept responsibility for the shipment,

(iii) Arrangements made for transfer of shipment security, and

(iv) Security arrangements at point where escorts accept responsibility for an import shipment.

(4) Hand-to-hand receipts shall be completed at origin and destination and at all points enroute where there is a transfer of custody.

(c) *Export/import shipments.* (1) A licensee who imports a formula quantity of strategic special nuclear material shall make arrangements to assure that the material will be protected in transit as follows:

(i) An individual designated by the licensee or his agent, or as specified by a contract of carriage, shall confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.

(ii) The shipment must be protected at all times within the geographical limits of the United States as provided in this section and §§ 73.25 and 73.27. The licensee shall retain each record required by these sections for three years after the close of period for which the licensee possesses the special nuclear material under each license authorizing the licensee to ship this material, and superseded material for three years after each change.

(2) A licensee who exports a formula quantity of strategic special nuclear material shall comply with the requirements of this section and §§ 73.25 and 73.27, as applicable, up to the first point where the shipment is taken off the transport outside the United States. The licensee shall retain each record required by these sections for three years after the close of period for which the licensee possesses the special nuclear material under each license authorizing the licensee to export this material, and superseded material for three years after each change.

(d) *Security organization.* (1) The licensee or his agent shall establish a transportation security organization, including armed escorts, armed response personnel or guards, and a movement control center manned and equipped to monitor and control shipments, to communicate with local law enforcement authorities, and to respond to safeguards contingencies.

(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 on duty at the movement control center during the course of any shipment.

(3) The licensee or the licensee's agent shall establish, maintain, and follow a written management system to provide for the development, revision, implementation, and enforcement of transportation physical protection procedures. The licensee or the agent shall retain as a record the current management system for three years after the close of period for which the licensee possesses the special nuclear material under the license for which the system was developed and, if any portion of the system is superseded, retain the superseded material for three years after each change. The system shall include:

(i) Written security procedures which document the structure of the transportation security organization and which detail the duties of drivers and escorts and other individuals responsible for security; and

(ii) Provision for written approval of such procedures and any revisions thereto by the individual with overall responsibility for the security function.

(4) Neither the licensee nor the licensee's agent shall permit an individual to act as an escort or other security organization member unless the individual has been trained, equipped, and qualified to perform each assigned security job duty in accordance with appendix B, of this part, ''General Criteria for Security Personnel.'' Upon the request of an authorized representative of the Commission, the licensee or the agent shall demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities. Armed escorts shall requalify in accordance with appendix B to this part at least every 12 months. Each requalification must be documented. The licensee or the agent shall retain documentation of the initial qualification for the term of employment and of each requalification as a record for three years from the date of the requalification.

(5) Armed escort and armed response force personnel armament shall include handguns, shotguns, and semiautomatic rifles, as described in appendix B to this part.

(e) *Contingency and Response Plans and Procedures.* (1) The licensee or the licensee's agent shall establish, maintain, and follow a written safeguards contingency plan for dealing with threats, thefts, and radiological sabotage related to strategic special nuclear material in transit subject to the provisions of this section. This safeguards contingency plan must be in accordance with the criteria in appendix C of this part, ''Licensee Safeguards Contingency Plan.'' The licensee or the agent shall retain the contingency plan as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the plan is used and superseded material for three years after each change.

(2) Upon detection of abnormal presence or activity of persons or vehicles attempting to penetrate a moving convoy or persons attempting to gain access to a parked cargo vehicle or upon evidence or indication of penetration of the cargo vehicle the armed escorts or other armed response personnel 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) Making the necessary tactical moves to prevent or impede acts of radiological sabotage or theft of strategic special nuclear material, and

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

(3) The licensee or his agent shall instruct every armed escort and all armed response personnel to prevent or impede acts of radiological sabotage or theft of strategic special material by using sufficient force to counter the force directed at him including the use of deadly force when armed escorts or armed response personnel have a reasonable belief that it is necessary in self-defense or in the defense of others.

(f) *Transfer and storage of strategic special nuclear material for domestic shipments.* (1) Strategic special nuclear material shall be placed in a protected area at transfer points if transfer is not immediate from one transport to another. Where a protected area is not available a controlled access area shall be established for the shipment. The transport may serve as a controlled access area.

(2) All transfers shall be protected by at least seven armed escorts or other armed personnel—one of whom shall serve as commander. At least five of the armed personnel (including the commander) shall be available to protect the shipment and at least three of the five shall keep the strategic special nuclear material under continuous surveillance while it is at the transfer point. The two remaining armed personnel shall take up positions at a remote monitoring location. The remote location may be a radio-equipped vehicle or a nearby place, apart from the shipment area, so that a single act cannot remove the capability of the personnel protecting the shipment for calling for assistance. Each of the seven armed escorts or other armed personnel shall be capable of maintaining communication with each other. The commander shall have the capability to communicate with the personnel at the remote location and with local law enforcement agencies for

emergency assistance. In addition, the armed escort personnel at the remote location shall have the capability to communicate with the law enforcement agencies and with the shipment movement control center. The commander shall call the remote location at least every 30 minutes to report the status of the shipment. If the calls are not received within the prescribed time, the personnel in the remote location shall request assistance from the law enforcement authorities, notify the shipment movement control center and initiate the appropriate contingency plans. Armed escorts or other armed personnel shall observe the opening of the cargo compartment of the incoming transport and ensure that the shipment is complete by checking locks and seals. A shipment loaded onto or transferred to another transport shall be checked to assure complete loading or transfer. Continuous visual surveillance of the cargo compartment shall be maintained up to the time the transport departs from the terminal. The escorts shall observe the transport until it has departed and shall notify the licensee or his agent of the latest status immediately thereafter.

(g) *Access control subsystems and procedures.* (1) A numbered picture badge identification procedure shall be used to identify all individuals who will have custody of a shipment. The identification procedure shall require that the individual who has possession of the strategic special nuclear material shall have, in advance, identification picture badges of all individuals who are to assume custody for the shipment. The shipment shall be released only when the individual who has possession of strategic special nuclear material has assured positive identification of all of the persons assuming custody for the shipment by comparing the copies of the identification badges that have been received in advance to the identification badges carried by the individuals who will assume custody of the shipment.

(2) Access to protected areas, controlled access areas, transports, escort vehicles, aircraft, rail cars, and containers where strategic special nuclear material is located shall be limited to individuals who have been properly identified and have been authorized access to these areas.

(3) Strategic special nuclear material shall be shipped in containers that are protected by tamper-indicating seals. The containers also shall be locked if they are not in another locked container or transport. The outermost container or transport also shall be protected by tamper-indicating seals.

(h) *Test and maintenance programs.* The licensee or his agent shall establish, maintain and follow a test and maintenance program for communications equipment and other physical protection related devices and equipment used pursuant to this section which shall include the following:

(1) Tests and inspections shall be conducted during the installation, and construction of physical protection related subsystems and components to assure that they comply with their respective design criteria and performance specifications.

(2) Preoperational tests and inspections shall be conducted for physical protection related subsystems and components to demonstrate their effectiveness, availability, and reliability with respect to their respective design criteria and performance specifications.

(3) Operational tests and inspections shall be conducted for physical protection related subsystems and components to assure their maintenance in an operable and effective condition.

(4) Preventive maintenance programs shall be established for physical protection related subsystems and components to assure their continued maintenance in an operable and effective condition.

(5) All physical protection related subsystems and components shall be maintained in operable condition. Corrective action procedures and compensatory measures shall be developed and employed to assure that the effectiveness of the physical protection system is not reduced by any single failure or other contingencies affecting the operation of the physical protection related equipment or structures.

(6) The transportation security program must be reviewed at least every 12 months by individuals independent of both security program management

and personnel who have direct responsibility for implementation of the security program. The review must include an audit of transportation security procedures and practices, an evaluation of the effectiveness of the transportation physical protection system, an audit of the transportation 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 review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, must be documented in a report to the responsible organization management 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.

(i) *Shipment by road.* (1) A detailed route plan shall be prepared which shows the routes to be taken, the refueling and rest stops, and the call-in times to the movement control center. All shipments shall be made on primary highways with minimum use of secondary roads. All shipments shall be made without intermediate stops except for refueling, rest or emergency stops.

(2) Cargo compartments of the trucks or trailers shall be locked and protected by tamper-indicating seals.

(3) The shipment shall be protected by one of the following methods:

(i) A specially designed cargo vehicle truck or trailer that reduces the vulnerability to theft. Design features of the truck or trailer shall permit immobilization of the truck or of the cargo-carrying portion of the vehicle and shall provide a deterrent to physical penetration of the cargo compartment. Two separate escort vehicles shall accompany the cargo vehicle. There shall be a total of seven armed escorts with at least two in the cargo vehicle. Escorts may also operate the cargo and escort vehicles.

(ii) An armored car cargo vehicle. Three separate escort vehicles shall accompany such a cargo vehicle. There shall be a total of seven armed escorts, with at least two in the cargo vehicle. Escorts may also operate the cargo and escort vehicles.

(4) All escort vehicles shall be bullet-resisting.

(5) Procedures shall be established to assure that no unauthorized persons or materials are on the cargo vehicle before strategic special nuclear material is loaded, or on the escort vehicles, immediately before the trip begins.

(6) Cargo and escort vehicles shall maintain continuous intraconvoy two-way communication. In addition at least two of the vehicles shall be equipped with radio telephones having the capability of communicating with the movement control center. A redundant means of communication shall also be available. Calls to the movement control center shall be made at least every half hour to convey the status and position of the shipment. In the event no call is received in accordance with these requirements, the licensee or his agent shall immediately notify the law enforcement authorities and the Director, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response, and initiate the appropriate contingency plan.

(7) At refueling, rest, or emergency stops at least seven armed escorts or other armed personnel shall be available to protect the shipment and at least three armed escorts or other armed personnel shall maintain continuous visual surveillance of the cargo compartment.

(8) Transfers to and from other modes of transportation shall be in accordance with paragraph (f) of this section.

(j) *Shipment by air.* (1) All shipments on commercial cargo aircraft shall be accompanied by two armed escorts who shall be able to converse in a common language with the captain of the aircraft.

(2) Transfers of these shipments shall be minimized and shall be conducted in accordance with paragraph (f) of this section. Such shipments shall be scheduled so that the strategic special nuclear material is loaded last and unloaded first.

(3) At scheduled stops, at least seven armed escorts or other armed personnel shall be available to protect the shipment and at least three armed escorts or other armed personnel shall maintain continuous visual surveillance of the cargo compartment.

(4) Export shipments shall be accompanied by two armed escorts from the last terminal in the United States until the shipment is unloaded at a foreign terminal and primary responsibility for physical protection is assumed by agents of the consignee. While on foreign soil, the escorts may surrender their weapons to legally constituted local authorities. After leaving the last terminal in the United States the shipment shall be scheduled with no intermediate stops.

(5) Import shipments shall be accompanied by two armed escorts at all times within the geographical limits of the United States. These escorts shall provide physical protection for the shipment until relieved by verified agents of the U.S. consignee.

(6) Procedures shall be established to assure that no unauthorized persons or material are on the aircraft before strategic special nuclear material is loaded on board.

(7) Arrangements shall be made at all domestic airports to assure that the seven required armed escorts or other armed personnel are available and that the required security measures will be taken upon landing.

(8) Arrangements shall be made at the foreign terminal at which the shipment is to be unloaded to assure that security measures will be taken on arrival.

(k) *Shipment by rail.* (1) A shipment by rail shall be escorted by seven armed escorts in the shipment car or an escort car next to the shipment car of the train. At least three escorts shall keep the shipment car under continuous visual surveillance. Escorts shall detrain at stops when practicable and time permits to maintain the shipment cars under continuous visual surveillance and to check car or container locks and seals.

(2) Procedures shall be established to assure that no unauthorized persons or materials are on the shipment or escort car before strategic special nuclear material is loaded on board.

(3) Only containers weighing 5,000 lbs or more shall be shipped on open rail cars.

(4) A voice communication capability between the escorts and the movement control center shall be maintained. A redundant means of continuous communication also shall be available. Calls to the movement control center shall be made at least every half hour to convey the status and position of the shipment. In the event no call is received in accordance with these requirements, the licensee or his agent shall immediately notify the law enforcement authorities and the appropriate Nuclear Regulatory Commission Regional Office listed in appendix A of this part and initiate their contingency plan.

(5) Transfer to and from other modes of transportation shall be in accordance with paragraph (f) of this section.

(l) *Shipment by sea.* (1) Shipments shall be made only on container-ships. The strategic special nuclear material container(s) shall be loaded into exclusive use cargo containers conforming to American National Standards Institute (ANSI) Standard MH5.1—''Basic Requirements for Cargo Containers'' (1971) or International Standards Organization (ISO) 1496, ''General Cargo Containers'' (1978). Locks and seals shall be inspected by the escorts whenever access is possible. The ANSI Standard MH5.1 (1971) and the (ISO) 1496 (1978), have been approved for incorporation by reference by the Director of the Federal Register. A copy of each of these standards is available for inspection at the NRC Library, 11545 Rockville Pike, Rockville, Maryland 20852-2738.

(2) All shipments shall be accompanied by two armed escorts who shall be able to converse in a common language with the captain of the ship.

(3) Minimum domestic ports of call shall be scheduled and there shall be no scheduled transfer to other vessels after the shipment leaves the last port in the United States. Transfer to and from other modes of transportation shall be in accordance with paragraph (f) of this section.

(4) At all ports of call the escorts shall ensure that the shipment is not removed. At least two armed escorts or other armed personnel shall maintain continuous visual surveillance of the cargo area where the container is stored up to the time the ship departs.

(5) Export shipments shall be accompanied by two armed escorts from the last port in the United States until the shipment is unloaded at a foreign terminal and prime responsibility for physical protection is assumed by agents of the consignee. While on foreign soil, the escorts may surrender their weapons to legally constituted local authorities.

(6) Import shipments shall be accompanied by two armed escorts at all times within the geographical limits of the United States. These escorts shall provide physical protection for the shipment until relieved by verified agents of the U.S. consignee.

(7) Ship-to-shore communications shall be available, and a ship-to-shore contact shall be made every six hours to relay position information, and the status of the shipment.

(8) Arrangements shall be made at the foreign terminals at which the shipment is to be unloaded to assure that security measures will be taken upon arrival.

[44 FR 68190, Nov. 28, 1979, as amended at 46 FR 2025, Jan. 8, 1981; 53 FR 19257, May 27, 1988; 57 FR 33430, July 29, 1992; 57 FR 61787, Dec. 29, 1992; 59 FR 50689, Oct. 5, 1994; 67 FR 3586, Jan. 25, 2002; 68 FR 14530, Mar. 26, 2003; 68 FR 23575, May 5, 2003; 74 FR 62684, Dec. 1, 2009; 83 FR 58723, Nov. 21, 2018]

§ 73.27 Notification requirements.

(a)(1) A licensee who delivers formula quantities of strategic special nuclear material to a carrier for transport shall immediately notify the consignee by telephone, telegraph, or teletype, of the time of departure of the shipment, and shall notify or confirm with the consignee the method of transportation, including the names of carriers, and the estimated time of arrival of the shipment at its destination.

(2) In the case of a shipment (f.o.b.) the point where it is delivered to a carrier for transport, a licensee shall, before the shipment is delivered to the carrier, obtain written certification from the licensee who is to take delivery of the shipment at the f.o.b. point that the physical protection arrangements required by §§ 73.25 and 73.26 for licensed shipments have been made. When a contractor exempt from the requirements for a Commission license is the consignee of a shipment, the licensee shall, before the shipment is delivered to the carrier, obtain written certification from the contractor who is to take delivery of the shipment at the f.o.b. point that the physical protection arrangements required by the United States Department of Energy Order Nos. 5632.1 or 5632.2, as appropriate, have been made.

(3) A licensee who delivers formula quantities of strategic special nuclear material to a carrier for transport or releases such special nuclear material f.o.b. at the point where it is delivered to a carrier for transport shall also make arrangements with the consignee to be notified immediately by telephone and telegraph, teletype, or cable, of the arrival of the shipment at its destination or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination.

(b) Each licensee who receives a shipment of formula quantities of strategic special nuclear material shall immediately notify by telephone and telegraph or teletype, the person who delivered the material to a carrier for transport and the Director, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response, of the arrival of the shipment at its destination. When a United States Department of Energy license-exempt contractor is the consignee, the licensee who is the consignor shall notify by telephone and telegraph, or teletype, the Director, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response of the arrival of the shipment at its destination immediately upon being notified of the receipt of the shipment by the license-exempt contractor as arranged pursuant to paragraph (a)(3) of this section. In the event such a shipment fails to arrive at its destination at the estimated time, or in the case of an export shipment, the licensee who exported the shipment,

shall immediately notify by telephone and telegraph or teletype, the Director, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response, and the licensee or other person who delivered the material to a carrier for transport. The licensee who made the physical protection arrangements shall also immediately notify by telephone and telegraph, or teletype, the Director, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response of the action being taken to trace the shipment.

(c) Each licensee who makes arrangements for physical protection of a shipment of formula quantities of strategic special nuclear material as required by §§ 73.25 and 73.26 shall immediately conduct a trace investigation of any shipment that is lost or unaccounted for after the estimated arrival time and file a report with the Commission as specified in §§ 73.1200 and 73.1205.

[44 FR 68192, Nov. 28, 1979, as amended at 67 FR 3586, Jan. 25, 2002; 68 FR 14530, Mar. 26, 2003; 68 FR 23575, May 5, 2003; 74 FR 62684, Dec. 1, 2009; 83 FR 58723, Nov. 21, 2018; 88 FR 15890, Mar. 14, 2023]

§ 73.28 Security background checks for secure transfer of nuclear materials.

Licensees are excepted from the security background check provisions in Section 170I of the AEA if they have not received Orders from the Nuclear Regulatory Commission containing requirements for background checks for trustworthiness and reliability that include fingerprinting and criminal history record checks as a prerequisite for unescorted access to radioactive materials.

[72 FR 3027, Jan. 24, 2007]

§ 73.35 Requirements for physical protection of irradiated reactor fuel (100 grams or less) in transit.

Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a quantity of irradiated reactor fuel weighing 100 grams (0.22 pounds) or less in net weight of irradiated fuel, exclusive of cladding or other structural or packaging material, which has a total external radiation level in excess of 1 Gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surface without intervening shielding, shall follow the physical protection requirements for category 1 quantities of radioactive material in subpart D of part 37 of this chapter.

[78 FR 17021, Mar. 19, 2013, as amended at 86 FR 43402, Aug. 9, 2021]

§ 73.37 Requirements for physical protection of irradiated reactor fuel in transit.

(a) *Performance objectives.* (1) Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a quantity of irradiated reactor fuel[1] in excess of 100 grams (0.22 lbs) in net weight of irradiated fuel, exclusive of cladding or other structural or packaging material, which has a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surface without intervening shielding, shall establish and maintain, or make arrangements for, and assure the proper implementation of, a physical protection system for shipments of such material that will achieve the following objectives:

(i) Minimize the potential for theft, diversion, or radiological sabotage of spent nuclear fuel shipments; and

(ii) Facilitate the location and recovery of spent nuclear fuel shipments that may have come under the control of unauthorized persons.

(2) To achieve these objectives, the physical protection system shall:

(i) Provide for early detection and assessment of attempts to gain unauthorized access to, or control over, spent nuclear fuel shipments;

(ii) Delay and impede attempts at theft, diversion, or radiological sabotage of spent nuclear fuel shipments; and

(iii) Provide for notification to the appropriate response forces of any attempts at theft, diversion, or radiological sabotage of a spent nuclear fuel shipment.

[1] For purposes of 10 CFR 73.37, the terms ''irradiated reactor fuel'' and ''spent nuclear fuel'' are used interchangeably.

(b) *General requirements.* To achieve the performance objectives of paragraph (a) of this section, a physical protection system established and maintained, or arranged for, by the licensee shall include the following elements:

(1) *Preplan and coordinate spent nuclear fuel shipments.* Each licensee shall:

(i) Ensure that each armed escort, as defined in §73.2, is instructed on the use of force sufficient to counter the force directed at the person, including the use of deadly force when the armed escort 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 Federal and State laws. This deadly force training requirement does not apply to members of local law enforcement agencies (LLEAs) performing escort duties for spent nuclear fuel shipments.

(ii) Preplan and coordinate shipment itineraries to ensure that the receiver at the final delivery point is present to accept the shipment.

(iii) Ensure written certification of any transfer of custody.

(iv) Preplan and coordinate shipment information no later than 2 weeks prior to the shipment or prior to the first shipment of a series of shipments with the governor of a State, or the governor's designee, of a shipment of spent nuclear fuel through or across the boundary of the State, in order to:

(A) Minimize intermediate stops and delays;

(B) Arrange for State law enforcement escorts;

(C) Arrange for positional information sharing when requested; and

(D) Develop route information, including the identification of safe havens.

(v) Arrange with local law enforcement authorities along the shipment route, including U.S. ports where vessels carrying spent nuclear fuel shipments are docked, for their response to a security-related emergency or a call for assistance.

(vi) Preplan and coordinate with the NRC to obtain advance approval of the routes used for road and rail shipments of spent nuclear fuel, and of any U.S. ports where vessels carrying spent nuclear fuel shipments are scheduled to stop. In addition to the requirements of this section, routes used for shipping spent nuclear fuel shall comply with the applicable requirements of the DOT regulations in Title 49 of the *Code of Federal Regulations* (49 CFR), in particular those identified in §71.5 of this chapter. The advance approval application shall provide:

(A) For road shipments, the route shall include locations of safe havens that have been coordinated with the appropriate State(s).

(B) The NRC approval shall be obtained prior to the 10-day advance notification requirement in §73.72 of this part.

(C) Information to be supplied to the NRC shall include, but is not limited to, the following:

(*1*) Shipper, consignee, carriers, transfer points, modes of shipment; and

(*2*) A statement of shipment security arrangements, including, if applicable, points where armed escorts transfer responsibility for the shipment.

(vii) Document the preplanning and coordination activities.

(viii) Ensure the protection of Safeguards Information relative to spent nuclear fuel in transit in accordance with §§73.21 and 73.22 of this part, especially the information described in §73.22(a)(2), which would include, at a minimum, the protection of the following information:

(A) The preplanning and coordination activities;

(B) Transportation physical security plan;

(C) Schedules and itineraries for specific spent nuclear fuel shipments until the information is no longer controlled as Safeguards Information, that is until at least 10 days after the shipment has entered or originated within the state; or for the case of a shipment in a series of shipments whose schedules are related, a statement that schedule information must be protected until 10 days after the last shipment in the series has entered or originated within the state and an estimate of the date on which the last shipment in the series will enter or originate within the state;

(D) Vehicle immobilization features, intrusion alarm devices, and communications;

(E) Arrangements with and capabilities of local police response forces, and locations of safe havens identified along the transportation route;

(F) Limitations of communications during transport;

(G) Procedures for response to security contingency events;

(H) Information concerning the tactics and capabilities required to defend against attempted sabotage, or theft and diversion of irradiated reactor fuel, or related information; and

(I) Engineering or safety analyses, security-related procedures or scenarios and other information related to the protection of the transported material if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of spent nuclear fuel in transit.

(2) *Advance notifications.* Prior to the shipment of spent nuclear fuel moving through or across the boundary of any State, outside the confines of the licensee's facility or other place of use or storage, a licensee subject to this section shall provide notification to the NRC, under § 73.72 of this part, and the governor of the State(s), or the governor's designee(s), of the spent nuclear fuel shipment. After June 11, 2013, the compliance date of the Tribal notification final rule, a licensee subject to this section shall notify the Tribal official or Tribal official's designee of each participating Tribe referenced in § 71.97(c)(3) of this chapter prior to the transport of spent fuel within or across the Tribal reservation. Contact information for each State, including telephone and mailing addresses of governors and governors' designees, and participating Tribes, including telephone and mailing addresses of Tribal officials and Tribal official's designees, is available on the NRC Web site at: *https://scp.nrc.gov/special/designee.pdf*''. A list of the contact information is also available upon request from the Director, Division of Materials Safety, Security, State, and Tribal Programs, U.S. Nuclear Regulatory Commission, Washington, DC 20555. The licensee shall comply with the following criteria in regard to each notification:

(i) *Procedures for submitting advance notification.* (A) The notification must be in writing and sent to the office of each appropriate governor or the governor's designee and each appropriate Tribal official or the Tribal official's designee.

(B) A notification delivered by mail must be postmarked at least 10 days before transport of a shipment within or through the State or Tribal reservation.

(C) A notification delivered by any other method must reach the office of the governor or the governor's designee and any Tribal official or Tribal official's designee at least 7 days before transport of a shipment within or through the State.

(ii) *Information to be furnished in advance notification of shipment.* The notification must include the following information:

(A) The name, address, and telephone number of the shipper, carrier and receiver of the shipment and the license number of the shipper and receiver;

(B) A description of the shipment as specified by DOT in 49 CFR 172.202 and 172.203(d); and

(C) A listing of the routes to be used within the State or Tribal reservation.

(iii) *Separate enclosure.* The licensee shall provide the following information, under § 73.22(f)(1), in a separate enclosure to the written notification:

(A) The estimated date and time of departure from the point of origin of the shipment;

(B) The estimated date and time of entry into the State or Tribal reservation;

(C) The estimated date and time of arrival of the shipment at the destination;

(D) For the case of a single shipment whose schedule is not related to the schedule of any subsequent shipment, a statement that schedule information must be protected under the provisions of §§ 73.21 and 73.22 until at least 10 days after the shipment has entered or originated within the State or Tribal reservation; and

(E) For the case of a shipment in a series of shipments whose schedules are related, a statement that schedule information must be protected under the provisions of §§ 73.21 and 73.22 of this part until 10 days after the last shipment in the series has entered or originated within the State or Tribal reservation, and an estimate of the date on which the last shipment in the series will enter or originate within the State or Tribal reservation.

(iv) *Revision notice.* A licensee shall notify by telephone a responsible individual in the office of the governor or in the office of the governor's designee and the office of the Tribal official or in the office of the Tribal official's designee of any schedule change that differs by more than 6 hours from the schedule information previously furnished under paragraph (b)(2)(iii) of this section, and shall inform that individual of the number of hours of advance or delay relative to the written schedule information previously furnished.

(v) *Cancellation notice.* Each licensee who cancels a shipment for which advance notification has been sent shall send a cancellation notice to the governor or to the governor's designee of each State previously notified, each Tribal official or the Tribal official's designee previously notified, and to the NRC's Director, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555. The licensee shall state in the notice that it is a cancellation and identify the advance notification that is being canceled.

(vi) *Records.* The licensee shall retain a copy of the preplanning and coordination activities, advance notification, and any revision or cancellation notice as a record for 3 years under § 73.70 of this part.

(3) *Transportation physical protection program.* (i) The transportation physical protection program established under paragraph (a)(1) of this section shall include armed escorts to protect spent nuclear fuel shipments and a movement control center, as defined in § 73.2 of this part, staffed and equipped to monitor and control spent nuclear fuel shipments, to communicate with local law enforcement authorities, and to respond to safeguards contingencies.

(ii) The movement control center must be staffed continuously by at least one individual who will actively monitor the progress of the spent nuclear fuel shipment and who has the authority to coordinate the physical protection activities.

(iii) The movement control center personnel must monitor the shipment continuously, *i.e.*, 24-hours per day, from the time the shipment commences, or if delivered to a carrier for transport, from the time of delivery of the shipment to the carrier, until safe delivery of the shipment at its final destination, and must immediately notify the appropriate agencies in the event of a safeguards event under the provisions of § 73.1200 of this part.

(iv) The movement control center personnel and the armed escorts must maintain a written log for each spent nuclear fuel shipment, which will include information describing the shipment and significant events that occur during the shipment. The log must be available for review by authorized NRC personnel for a period of at least 3 years following completion of the shipment.

(v) The licensee shall develop, maintain, revise and implement written transportation physical protection procedures which address the following:

(A) Access controls to ensure no unauthorized persons have access to the shipment and Safeguards Information;

(B) Roles and responsibilities of the movement control center personnel, drivers, armed escorts and other individuals relative to the security of the shipment;

(C) Reporting of safeguards events under § 73.1200 of this part;

(D) Communications protocols that include a strategy for the use of authentication and duress codes, the management of refueling or other stops, detours, and the loss of communications, temporarily or otherwise; and

(E) Normal conditions operating procedures.

(vi) The licensee shall retain as a record the transportation physical protection procedures for 3 years after the

close of period for which the licensee possesses the spent nuclear fuel.

(vii) The transportation physical protection program shall:

(A) Provide that escorts (other than members of local law enforcement agencies serving as armed escorts, or ship's officers serving as unarmed escorts) have successfully completed the training required by appendix D of this part, including the equivalent of the weapons training and qualifications program required of guards, as described in sections III and IV of appendix B of this part, to assure that each such individual is fully qualified to use the assigned weapons;

(B) Provide that shipment escorts communicate with the movement control center at random intervals, not to exceed 2 hours, to advise of the status of the shipment for road and rail shipments, and for sea shipments while shipment vessels are docked at U.S. ports; and

(C) Provide that at least one armed escort remains alert at all times, maintains constant visual surveillance of the shipment, and periodically reports to the movement control center at regular intervals not to exceed 30 minutes during periods when the shipment vehicle is stopped, or the shipment vessel is docked.

(viii)(A) The licensee must ensure that the firearms background check requirements of §73.17 are met for all armed escorts whose official duties require access to covered weapons or who inventory enhanced weapons.

(B) The provisions of this paragraph are only applicable to licensees subject to this section who are also subject to the firearms background check provisions of §73.17.

(C) The provisions of this paragraph are not applicable to members of local law enforcement agencies serving as armed escorts or ship's officers serving as unarmed escorts.

(4) *Contingency and response procedures.* (i) In addition to the procedures established under paragraph (b)(3)(v) of this section, the licensee shall establish, maintain, and follow written contingency and response procedures to address threats, thefts, and radiological sabotage related to spent nuclear fuel in transit.

(ii) The licensee shall ensure that personnel associated with the shipment shall be appropriately trained regarding contingency and response procedures.

(iii) The licensee shall retain the contingency and response procedures as a record for 3 years after the close of period for which the licensee possesses the spent nuclear fuel.

(iv) The contingency and response procedures must direct that, upon detection of the abnormal presence of unauthorized persons, vehicles, or vessels in the vicinity of a spent nuclear fuel shipment or upon detection of a deliberately induced situation that has the potential for damaging a spent nuclear fuel shipment, the armed escort will:

(A) Determine whether or not a threat exists;

(B) Assess the extent of the threat, if any;

(C) Implement the procedures developed under paragraph (b)(4)(i) of this section;

(D) Take the necessary steps to delay or impede threats, thefts, or radiological sabotage of spent nuclear fuel; and

(E) Inform local law enforcement agencies of the threat and request assistance without delay, but not to exceed 15 minutes after discovery.

(c) *Shipments by road.* In addition to the provisions of paragraph (b) of this section, the physical protection system for any portion of a spent nuclear fuel shipment by road shall provide that:

(1) The transport vehicle is:

(i) Occupied by at least two individuals, one of whom serves as an armed escort, and escorted by an armed member of the local law enforcement agency in a mobile unit of such agency; or

(ii) Led by a separate vehicle occupied by at least one armed escort, and trailed by a third vehicle occupied by at least one armed escort.

(2) As permitted by law, all armed escorts are equipped with a minimum of two weapons. This requirement does not apply to local law enforcement agency personnel who are performing escort duties.

(3) The transport vehicle and each escort vehicle are equipped with redundant communication abilities that provide 2-way communications between

the transport vehicle, the escort vehicle(s), the movement control center, local law enforcement agencies, and one another. To ensure that 2-way communication is possible at all times, alternate communications should not be subject to the same failure modes as the primary communication.

(4) The transport vehicle is equipped with NRC-approved features that permit immobilization of the cab or cargo-carrying portion of the vehicle.

(5) The transport vehicle driver has been familiarized with, and is capable of implementing, transport vehicle immobilization, communications, and other security procedures.

(6) Shipments are continuously and actively monitored by a telemetric position monitoring system or an alternative tracking system reporting to a movement control center. A movement control center shall provide positive confirmation of the location, status, and control over the shipment. The movement control center shall implement preplanned procedures in response to deviations from the authorized route or a notification of actual, attempted, or suspicious activities related to the theft, loss, diversion, or radiological sabotage of a shipment. These procedures shall include, but not be limited to, the identification of and contact information for the appropriate local law enforcement agency along the shipment route.

(d) *Shipments by rail.* In addition to the provisions of paragraph (b) of this section, the physical protection system for any portion of a spent nuclear fuel shipment by rail shall provide that:

(1) A shipment car is accompanied by two armed escorts (who may be members of a local law enforcement agency), at least one of whom is stationed at a location on the train that will permit observation of the shipment car while in motion.

(2) As permitted by law, all armed escorts are equipped with a minimum of two weapons. This requirement does not apply to local law enforcement agency personnel who are performing escort duties.

(3) The train operator(s) and each escort are equipped with redundant communication abilities that provide 2-way communications between the transport, the escort vehicle(s), the movement control center, local law enforcement agencies, and one another. To ensure that 2-way communication is possible at all times, alternate communications should not be subject to the same failure modes as the primary communication.

(4) Rail shipments are monitored by a telemetric position monitoring system or an alternative tracking system reporting to the licensee, third-party, or railroad movement control center. The movement control center shall provide positive confirmation of the location of the shipment and its status. The movement control center shall implement preplanned procedures in response to deviations from the authorized route or to a notification of actual, attempted, or suspicious activities related to the theft, diversion, or radiological sabotage of a shipment. These procedures shall include, but not be limited to, the identification of and contact information for the appropriate local law enforcement agency along the shipment route.

(e) *Shipments by U.S. waters.* In addition to the provisions of paragraph (b) of this section, the physical protection system for any portion of a spent nuclear fuel shipment traveling on U.S. waters shall provide that:

(1) A shipment vessel while docked at a U.S. port is protected by:

(i) Two armed escorts stationed on board the shipment vessel, or stationed on the dock at a location that will permit observation of the shipment vessel; or

(ii) A member of a local law enforcement agency, equipped with normal local law enforcement agency radio communications, who is stationed on board the shipment vessel, or on the dock at a location that will permit observation of the shipment vessel.

(2) As permitted by law, all armed escorts are equipped with a minimum of two weapons. This requirement does not apply to local law enforcement agency personnel who are performing escort duties.

(3) A shipment vessel while within U.S. territorial waters shall be accompanied by an individual, who may be an officer of the shipment vessel's crew, who will assure that the shipment is

unloaded only as authorized by the licensee.

(4) Each armed escort is equipped with redundant communication abilities that provide 2-way communications between the vessel, the movement control center, local law enforcement agencies, and one another. To ensure that 2-way communication is possible at all times, alternate communications should not be subject to the same failure modes as the primary communication.

(f) *Investigations.* Each licensee who makes arrangements for the shipment of spent nuclear fuel shall immediately conduct an investigation, in coordination with the receiving licensee, of any shipment that is lost or unaccounted for after the designated no-later-than arrival time in the advance notification.

(g) State officials, State employees, Tribal officials, Tribal employees, and other individuals, whether or not licensees of the NRC, who receive information of the kind specified in paragraph (b)(2)(iii) of this section and any other Safeguards Information as defined in § 73.22(a) of this part shall protect that information against unauthorized disclosure as specified in §§ 73.21 and 73.22 of this part.

[78 FR 29550, May 20, 2013, as amended at 79 FR 75741, Dec. 19, 2014; 80 FR 74981, Dec. 1, 2015; 83 FR 30288, June 28, 2018; 83 FR 58723, Nov. 21, 2018; 86 FR 43403, Aug. 9, 2021; 88 FR 15890, Mar. 14, 2023]

§ 73.38 Personnel access authorization requirements for irradiated reactor fuel in transit.

(a) *General.* (1) Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a quantity of spent nuclear fuel as described in § 73.37(a)(1) of this part shall comply with the requirements of this section, as appropriate, before any spent nuclear fuel is transported or delivered to a carrier for transport.

(2) Each licensee shall establish, implement, and maintain its access authorization program under the requirements of this section.

(i) Each licensee shall be responsible for the continuing effectiveness of the access authorization program.

(ii) Each licensee shall ensure that the access authorization program is reviewed at an appropriate frequency to confirm compliance with the requirements of this section and that prompt comprehensive actions are taken to correct any noncompliance that is identified.

(iii) The review shall evaluate all program performance objectives and requirements.

(iv) Each review report must document conditions that are adverse to the proper performance of the access authorization program, the cause of the condition(s), and when appropriate, recommended corrective actions, and corrective actions taken. The licensee shall review the audit findings and take any additional corrective actions necessary to preclude repetition of the condition, including reassessment of the deficient areas where indicated.

(3) By August 19, 2013, each licensee that is subject to this provision shall implement the requirements of this section through revisions to its physical security plan or transportation security plan.

(b) *General performance objective.* The licensee's access authorization program must ensure that the individuals specified in paragraph (c) 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.

(c) *Applicability.* (1) Licensees shall subject the following individuals to an access authorization program:

(i) Any individual to whom a licensee intends to grant unescorted access to spent nuclear fuel in transit, including employees of a contractor or vendor;

(ii) Any individual whose duties and responsibilities permit the individual to take actions by physical or electronic means that could adversely impact the safety, security, or emergency response to spent nuclear fuel in transit (*i.e.*, movement control personnel, vehicle drivers, or other individuals accompanying spent nuclear fuel shipments);

(iii) Any individual whose duties and responsibilities include implementing a licensee's physical protection program under § 73.37, including but not limited to, non-LLEA armed escorts;

(iv) Any individual whose assigned duties and responsibilities provide access to spent nuclear fuel shipment information that is considered to be Safeguards Information under § 73.22(a)(2); and

(v) The licensee access authorization program reviewing official.

(2) Fingerprinting, and the identification and criminal history records checks required by Section 149 of the Atomic Energy Act of 1954, as amended, and other elements of the background investigation are not required for the following individuals prior to granting access authorization relative to spent nuclear fuel in transit:

(i) Persons identified in §§ 73.59 and 73.61 of this part;

(ii) Federal, State, and local officials, including inspectors, whose occupational status are consistent with the promotion of common defense and security and the protection of public health and safety relative to spent nuclear fuel in transit;

(iii) Emergency response personnel who are responding to an emergency;

(iv) An individual who has had a favorably adjudicated U.S. Government criminal history records check within the last 5 years, under a comparable U.S. Government program involving fingerprinting and an FBI identification and criminal history records check (e.g. National Agency Check, Transportation Worker Identification Credentials (TWIC) under 49 CFR part 1572, Bureau of Alcohol Tobacco Firearms and Explosives background check and clearances under 27 CFR part 555, Health and Human Services security risk assessments for possession and use of select agents and toxins under 42 CFR part 73, Hazardous Material security threat assessment for hazardous material endorsement to commercial drivers license under 49 CFR part 1572, Customs and Border Patrol's Free and Secure Trade (FAST) Program) provided that he or she makes available the appropriate documentation. Written confirmation from the agency/employer that granted the Federal security clearance or reviewed the criminal history records check must be provided to the licensee. The licensee shall retain this documentation for a period of 3 years from the date the individual no longer requires access authorization relative to spent nuclear fuel in transit; and

(v) Any individual who has an active Federal security clearance, provided that he or she makes available the appropriate documentation. Written confirmation from the agency/employer that granted the Federal security clearance or reviewed the criminal history records check must be provided to the licensee. The licensee shall retain this documentation for a period of 3 years from the date the individual no longer requires access authorization relative to spent nuclear fuel in transit.

(d) *Background investigation.* Before allowing an individual to have unescorted access or access authorization relative to spent nuclear fuel[2] in transit the licensees shall complete a background investigation as defined in § 73.2 of this part of the individual seeking to have unescorted access or access authorization. The scope of the investigation must encompass at least the past 10 years, or if 10 years of information is not available then as many years in the past that information is available. The background investigation does not apply to Federal, State or local law enforcement personnel who are performing escort duties. The background investigation must include, but is not limited to, the following elements:

(1) *Informed consent.* Licensees 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 to whom the individual is applying for access authorization shall inform the individual of his or her right to review information collected to assure its accuracy, and provide the individual with an opportunity to correct any inaccurate or incomplete information that is developed by the licensee.

[2] For purposes of 10 CFR 73.38, the terms ''irradiated reactor fuel'' as described in 10 CFR 73.37 and ''spent nuclear fuel'' are used interchangeably.

(i) The subject individual may withdraw his or her consent at any time. Licensees shall inform the individual that:

(A) Withdrawal of his or her consent will remove the individual's application for access authorization under the licensee's access authorization program; and

(B) Other licensees shall have access to information documenting the withdrawal.

(ii) If an individual withdraws his or her consent, licensees may not initiate any elements of the background investigation that were not in progress at the time the individual withdrew his or her consent, but shall complete any background investigation elements that are in progress at the time consent is withdrawn. The licensee shall record the status of the individual's application for access authorization. Additionally, licensees shall collect and maintain the individual's application for access authorization; his or her withdrawal of consent for the background investigation; the reason given by the individual for the withdrawal; and any pertinent information collected from the background investigation elements that were completed. This information must be shared with other licensees under paragraph (l)(4) of this section.

(iii) Licensees shall inform, in writing, any individual who is applying for access authorization that the following actions are sufficient cause for denial or unfavorable termination of access authorization status:

(A) Refusal to provide a signed consent for the background investigation;

(B) Refusal to provide, or the falsification of, any personal history information required under this section, including the failure to report any previous denial or unfavorable termination of access authorization;

(C) Refusal to provide signed consent for the sharing of personal information with other licensees under paragraph (d)(5)(v) of this section; or

(D) Failure to report any arrests or legal actions specified in paragraph (f) of this section.

(2) *Personal history disclosure.* Any individual who is required to have a background investigation under this section shall disclose the personal history information that is required by the licensee's access authorization program for the reviewing official to make a determination of the individual's trustworthiness and reliability. Refusal to provide, or the falsification of, any personal history information required by this section is sufficient cause for denial or termination of access authorization.

(3) *Criminal history.* Fingerprinting and an FBI identification and criminal history records check under § 73.57 of this part.

(4) *Verification of true identity.* Licensees shall verify the true identity of an individual who is applying to have access authorization to ensure that the applicant is who they claim to be. A licensee shall review official identification documents (e.g., driver's license, passport, government identification, State, province, or country of birth issued certificate of birth) and compare the documents to personal information data provided by the individual to identify any discrepancy in the information. Licensees shall document the type, expiration, and identification number of the identification, or maintain a photocopy of identifying documents on file under § 73.38(c). Licensees shall certify and affirm in writing that the identification was properly reviewed and maintain the certification and all related documents for review upon inspection.

(5) *Employment history evaluation.* Licensees shall ensure that an employment history evaluation has been completed on a best effort basis, by questioning the individual's present and former employers, and by determining the activities of the individual while unemployed.

(i) For the claimed employment period, the individual must provide the reason for any termination, eligibility for rehire, and other information that could reflect on the individual's trustworthiness and reliability.

(ii) If the claimed employment was military service the individual shall provide a characterization of service, reason for separation, and any disciplinary actions that could affect a trustworthiness and reliability determination.

(iii) If education is claimed in lieu of employment, the individual shall provide any information related to the claimed education that could reflect on the individual's trustworthiness and reliability and, at a minimum, verify that the individual was registered for the classes and received grades that indicate that the individual participated in the educational process during the claimed period.

(iv) If a previous employer, educational institution, or any other entity with which the individual claims to have been engaged fails to provide information or indicates an inability or unwillingness to provide information within 3 business days of the request, the licensee shall:

(A) Document this refusal or unwillingness in the licensee's record of the investigation; and

(B) Obtain a confirmation of employment, educational enrollment and attendance, or other form of engagement claimed by the individual from at least one alternate source that has not been previously used.

(v) When any licensee is seeking the information required for an access authorization decision under this section and has obtained a signed release from the subject individual authorizing the disclosure of such information, other licensees shall make available the personal or access authorization information requested regarding the denial or unfavorable termination of an access authorization.

(vi) In conducting an employment history evaluation, the licensee may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or email. Licensees shall make a record of the contents of the telephone call and shall retain that record, and any documents or electronic files obtained electronically, under paragraph (l) of this section.

(6) *Credit history evaluation.* Licensees shall ensure the evaluation of the full credit history of any individual who is applying for access authorization relative to spent nuclear fuel in transit. A full credit history evaluation must include, but is not limited to, an inquiry to detect potential fraud or misuse of social security numbers or other financial identifiers, and a review and evaluation of all of the information that is provided by a national credit-reporting agency about the individual's credit history. For foreign nationals and U.S. citizens who have resided outside the U.S. and do not have established credit history that covers at least the most recent 7 years in the U.S., the licensee must document all attempts to obtain information regarding the individual's credit history and financial responsibility from some relevant entity located in that other country or countries.

(7) *Criminal history review.* The licensee shall evaluate the entire criminal history record of an individual who is applying for access authorization to determine whether the individual has a record of criminal activity that may adversely impact his or her trustworthiness and reliability. The scope of the applicant's criminal history review must cover all residences of record for the 10-year period preceding the date of application for access authorization.

(8) *Character and reputation determination.* Licensees shall ascertain the character and reputation of an individual who has applied for access authorization relative to spent nuclear fuel in transit by conducting reference checks. Reference checks may not be conducted with any person who is known to be a close member of the individual's family, including but not limited to, the individual's spouse, parents, siblings, or children, or any individual who resides in the individual's permanent household. The reference checks must focus on the individual's reputation for trustworthiness and reliability.

(9) *Corroboration.* The licensee shall also, to the extent possible, obtain independent information to corroborate that provided by the individual (e.g., seek references not supplied by the individual).

(e) *Determination of trustworthiness and reliability; Documentation.* (1) The licensee shall determine whether to grant, deny, unfavorably terminate, maintain, or administratively withdraw an individual's access authorization based on an evaluation of all of the information required by this section. The licensee may terminate or

administratively withdraw an individual's access authorization based on information obtained after the background investigation has been completed and the individual granted access authorization.

(2) The licensee may not permit any individual to have unescorted access or access authorization until all of the information required by this section has been evaluated by the reviewing official and the reviewing official has determined that the individual is trustworthy and reliable. The licensee may deny unescorted access or access authorization to any individual based on disqualifying information obtained at any time during the background investigation.

(f) *Protection of information.* (1) Licensees shall protect background investigation information from unauthorized disclosure.

(2) Licensees may not disclose the background investigation information collected and maintained to persons other than the subject individual, his/her representative, or to those who have a need to know in performing assigned duties related to the process of granting or denying unescorted access to spent nuclear fuel in transit. No individual authorized to have access to the information may re-disseminate the information to any other individual who does not have a need to know.

(3) The personal information obtained on an individual from a background investigation may be transferred to another licensee:

(i) Upon the individual's written request to the licensee holding the data to re-disseminate the information contained in his/her file; and

(ii) The acquiring licensee verifies information such as name, date of birth, social security number, sex, and other applicable physical characteristics for identification.

(4) The licensee shall make background investigation records obtained under this section available for examination by an authorized representative of the NRC to determine compliance with applicable laws and regulations.

(5) The licensee shall retain all fingerprint and criminal history records received from the FBI, or a copy if the file has been transferred, on an individual (including data indicating no record) for 5 years from the date the individual no longer requires unescorted access or access authorization relative to spent nuclear fuel in transit.

(g) *Grandfathering.* For purposes of this section, licensees are not required to obtain the fingerprints of any person who has been fingerprinted, pursuant to an NRC order or regulation, for an FBI identification and criminal history records check within the 5 years of the effective date of this rule.

(h) *Reinvestigations.* Licensees shall conduct fingerprinting and FBI identification and criminal history records check, a criminal history review, and credit history re-evaluation every 10 years for any individual who has unescorted access authorization to spent nuclear fuel in transit. The reinvestigations must be completed within 10 years of the date on which these elements were last completed and should address the 10 years following the previous investigation.

(i) *Self-reporting of legal actions.* (1) Any individual who has applied for an access authorization or is maintaining an access authorization under this section shall promptly report to the reviewing official, his or her supervisor, or other management personnel designated in licensee procedures any legal action(s) taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that requires a court appearance, including but not limited to an arrest, an indictment, the filing of charges, or a conviction, but excluding minor civil actions or misdemeanors such as parking violations or speeding tickets. The recipient of the report shall, if other than the reviewing official, promptly convey the report to the reviewing official. On the day that the report is received, the reviewing official shall evaluate the circumstances related to the reported legal action(s) and re-determine the reported individual's access authorization status.

(2) The licensee shall inform the individual of this obligation, in writing, prior to granting unescorted access or certifying access authorization.

(j) *Access authorization procedures.* (1) Licensees shall develop, implement, and maintain written procedures for conducting background investigations for persons who are applying for unescorted access or access authorization for spent nuclear fuel in transit.

(2) Licensees shall develop, implement, and maintain written procedures for updating background investigations for persons who are applying for reinstatement of unescorted access or access authorization.

(3) Licensees shall develop, implement, and maintain written procedures to ensure that persons who have been denied unescorted access or access authorization are not allowed access to spent nuclear fuel in transit or information relative to spent nuclear fuel in transit.

(4) Licensees shall develop, implement, and maintain written procedures for the notification of individuals who are denied unescorted access or access authorization for spent nuclear fuel in transit. The procedures shall include provisions for the review, at the request of the affected individual, of a denial or termination of unescorted access or access authorization. The procedure must contain a provision to ensure that the individual is informed of the grounds for the denial or termination of unescorted access or access authorization and allow the individual an opportunity to provide additional relevant information.

(k) *Right to correct and complete information.* (1) Prior to any final adverse determination, licensees shall provide each individual subject to this section with the right to complete, correct, and explain information obtained as a result of the licensee's background investigation. Confirmation of receipt by the individual of this notification must be maintained by the licensee for a period of 1 year from the date of the notification.

(2) If after reviewing their criminal history record an individual believes that it is incorrect or incomplete in any respect and wishes to change, correct, update, or explain anything in the record, the individual may initiate challenge procedures.

(l) *Records.* (1) The licensee shall retain documentation regarding the trustworthiness and reliability of individual employees for 5 years from the date the individual no longer requires unescorted access or access authorization relative to spent nuclear fuel in transit.

(2) The licensee shall retain a copy of the current access authorization program procedures as a record for 5 years after the procedure is no longer needed or until the Commission terminates the license, if the license is terminated before the end of the retention period. If any portion of the procedure is superseded, the licensee shall retain the superseded material for 5 years after the record is superseded.

(3) The licensee shall retain the list of persons approved for unescorted access or access authorization and the list of those individuals that have been denied unescorted access or access authorization for 5 years after the list is superseded or replaced.

(4) Licensees who have been authorized to add or manipulate data that is shared with licensees subject to this section shall ensure that data linked to the information about individuals who have applied for unescorted access or access authorization, which is specified in the licensee's access authorization program documents, is retained.

(i) If the shared information used for determining individual's trustworthiness and reliability changes or new or additional information is developed about the individual, the licensees that acquire this information shall correct or augment the data and ensure it is shared with licensees subject to this section. If the changed, additional or developed information has implications for adversely affecting an individual's trustworthiness and reliability, licensees who discovered or obtained the new, additional or changed information, shall, on the day of discovery, inform the reviewing official of any licensee access authorization program under which the individual is maintaining his or her unescorted access or access authorization status of the updated information.

(ii) The reviewing official shall evaluate the shared information and take appropriate actions, which may include denial or unfavorable termination of the individual's unescorted access or

access authorization. If the notification of change or updated information cannot be made through usual methods, licensees shall take manual actions to ensure that the information is shared as soon as reasonably possible. Records maintained in any database(s) must be available for the NRC review.

(5) If a licensee administratively withdraws an individual's unescorted access or access authorization status caused by a delay in completing any portion of the background investigation or for a licensee initiated evaluation, or re-evaluation that is not under the individual's control, the licensee shall record this administrative action to withdraw the individual's unescorted access or unescorted access authorization and shall share this information with other licensees subject to this section. However, licensees shall not document this administrative withdrawal as denial or unfavorable termination and shall not respond to a suitable inquiry conducted under the provisions of 10 CFR part 26, a background investigation conducted under the provisions of this section, or any other inquiry or investigation as denial nor unfavorable termination. Upon favorable completion of the background investigation element that caused the administrative withdrawal, the licensee shall immediately ensure that any matter that could link the individual to the administrative action is eliminated from the subject individual's access authorization or personnel record and other records, except if a review of the information obtained or developed causes the reviewing official to unfavorably terminate or deny the individual's unescorted access.

[78 FR 29553, May 20, 2013]

Subpart F—Physical Protection Requirements at Fixed Sites

SOURCE: 88 FR 15881, Mar. 14, 2023, unless otherwise noted.

§ 73.40 Physical protection: General requirements at fixed sites.

Each licensee shall provide physical protection at a fixed site, or contiguous sites where licensed activities are conducted, against radiological sabotage, or against theft of special nuclear material, or against both, in accordance with the applicable sections of this Part for each specific class of facility or material license. If applicable, the licensee shall establish and maintain physical security in accordance with security plans approved by the Nuclear Regulatory Commission.

[58 FR 13700, Mar. 15, 1993]

§ 73.45 Performance capabilities for fixed site physical protection systems.

(a) To meet the general performance requirements of § 73.20 a fixed site physical protection system shall include the performance capabilities described in paragraphs (b) through (g) of this section unless otherwise authorized by the Commission.

(b) Prevent unauthorized access of persons, vehicles and materials into material access areas and vital areas. To achieve this capability the physical protection system shall:

(1) Detect attempts to gain unauthorized access or introduce unauthorized material across material access or vital area boundaries by stealth or force using the following subsystems and subfunctions:

(i) Barriers to channel persons and material to material access and vital area entry control points and to delay any unauthorized penetration attempts by persons or materials sufficient to assist detection and permit a response that will prevent the penetration; and

(ii) Access detection subsystems and procedures to detect, assess and communicate any unauthorized penetration attempts by persons or materials at the time of the attempt so that the response can prevent the unauthorized access or penetration.

(2) Detect attempts to gain unauthorized access or introduce unauthorized materials into material access areas or vital areas by deceit using the following subsystems and subfunctions:

(i) Access authorization controls and procedures to provide current authorization schedules and entry criteria for both persons and materials; and

(ii) Entry controls and procedures to verify the identity of persons and materials and assess such identity against current authorization schedules and

entry criteria before permitting entry and to initiate response measures to deny unauthorized entries.

(c) Permit only authorized activities and conditions within protected areas, material access areas, and vital areas. To achieve this capability the physical protection system shall:

(1) Detect unauthorized activities or conditions within protected areas, material access areas and vital areas using the following subsystems and subfunctions:

(i) Controls and procedures that establish current schedules of authorized activities and conditions in defined areas;

(ii) Boundaries to define areas within which the authorized activities and conditions are permitted; and

(iii) Detection and surveillance subsystems and procedures to discover and assess unauthorized activities and conditions and communicate them so that response can be such as to stop the activity or correct the conditions to satisfy the general performance objective and requirements of § 73.20(a).

(d) Permit only authorized placement and movement of strategic special nuclear material within material access areas. To achieve this capability the physical protection system shall:

(1) Detect unauthorized placement and movement of strategic special nuclear material within the material access area using the following subsystems and subfunctions:

(i) Controls and procedures to delineate authorized placement and control for strategic special nuclear material;

(ii) Controls and procedures to establish current authorized placement and movement of all strategic special nuclear material within material access areas;

(iii) Controls and procedures to maintain knowledge of the identity, quantity, placement, and movement of all strategic special nuclear material within material access areas; and

(iv) Detection and monitoring subsystems and procedures to discover and assess unauthorized placement and movement of strategic special nuclear material and communicate them so that response can be such as to return the strategic special nuclear material to authorized placement or control.

(e) Permit removal of only authorized and confirmed forms and amounts of strategic special nuclear material from material access areas. To achieve this capability the physical protection system shall:

(1) Detect attempts at unauthorized removal of strategic special nuclear material from material access areas by stealth or force using the following subsystems and subfunctions:

(i) Barriers to channel persons and materials exiting a material access area to exit control points and to delay any unauthorized strategic special nuclear material removal attempts sufficient to assist detection and assessment and permit a response that will prevent the removal; and satisfy the general performance objective and requirements of § 73.20(a); and

(ii) Detection subsystems and procedures to detect, assess and communicate any attempts at unauthorized removal of strategic special nuclear material so that response to the attempt can be such as to prevent the removal and satisfy the general performance objective and requirements of § 73.20(a).

(2) Confirm the identity and quantity of strategic special nuclear material presented for removal from a material access area and detect attempts at unauthorized removal of strategic special nuclear material from material access areas by deceit using the following subsystems and subfunctions:

(i) Authorization controls and procedures to provide current schedules for authorized removal of strategic special nuclear material which specify the authorized properties and quantities of material to be removed, the persons authorized to remove the material, and the authorized time schedule;

(ii) Removal controls and procedures to identify and confirm the properties and quantities of material being removed and verify the identity of the persons making the removal and time of removal and assess these against the current authorized removal schedule before permitting removal; and

(iii) Communications subsystems and procedures to provide for notification of an attempted unauthorized or unconfirmed removal so that response can be such as to prevent the removal

and satisfy the general performance objective and requirements of § 73.20(a).

(f) Provide for authorized access and assure detection of and response to unauthorized penetrations of the protected area to satisfy the general performance objective and requirements of § 73.20(a). To achieve this capability the physical protection system shall:

(1) Detect attempts to gain unauthorized access or introduce unauthorized persons, vehicles, or materials into the protected area by stealth or force using the following subsystems and subfunctions:

(i) Barriers to channel persons, vehicles, and materials to protected area entry control points; and to delay any unauthorized penetration attempts or the introduction of unauthorized vehicles or materials sufficient to assist detection and assessment and permit a response that will prevent the penetration or prevent such penetration and satisfy the general performance objective and requirements of § 73.20(a); and

(ii) Access detection subsystems and procedures to detect, assess and communicate any unauthorized access or penetrations or such attempts by persons, vehicles, or materials at the time of the act or the attempt so that the response can be such as to prevent the unauthorized access or penetration, and satisfy the general performance objective and requirements of § 73.20(a).

(2) Detect attempts to gain unauthorized access or introduce unauthorized persons, vehicles, or materials into the protected area by deceit using the following subsystems and subfunctions:

(i) Access authorization controls and procedures to provide current authorization schedules and entry criteria for persons, vehicles, and materials; and

(ii) Entry controls and procedures to verify the identity of persons, materials and vehicles and assess such identity against current authorization schedules before permitting entry and to initiate response measures to deny unauthorized access.

(g) *Response.* Each physical protection program shall provide a response capability to assure that the five capabilities described in paragraphs (b) through (f) of this section are achieved and that adversary forces will be engaged and impeded until offsite assistance forces arrive. To achieve this capability a licensee shall:

(1) Establish a security organization to:

(i) Provide trained and qualified personnel to carry out assigned duties and responsibilities; and

(ii) Provide for routine security operations and planned and predetermined response to emergencies and safeguards contingencies.

(2) Establish a predetermined plan to respond to safeguards contingency events.

(3) Provide equipment for the security organization and facility design features to:

(i) Provide for rapid assessment of safeguards contingencies;

(ii) Provide for response by assigned security organization personnel which is sufficiently rapid and effective to achieve the predetermined objective of the response; and

(iii) Provide protection for the assessment and response personnel so that they can complete their assigned duties.

(4) Provide communications networks to:

(i) Transmit rapid and accurate security information among onsite forces for routine security operation, assessment of a contingency, and response to a contingency; and

(ii) Transmit rapid and accurate detection and assessment information to offsite assistance forces.

(5) Assure that a single adversary action cannot destroy the capability of the security organization to notify offsite response forces of the need for assistance.

[44 FR 68193, Nov. 28, 1979]

§ 73.46 Fixed site physical protection systems, subsystems, components, and procedures.

(a) A licensee physical protection system established pursuant to the general performance objective and requirements of § 73.20(a) and the performance capability requirements of § 73.45 shall include, but are not necessarily limited to, the measures specified in paragraphs (b) through (h) of this section. The Commission may require, depending on individual facility

and site conditions, alternate or additional measures deemed necessary to meet the general performance objective and requirements of § 73.20. The Commission also may authorize protection measures other than those required by this section if, in its opinion, the overall level of performance meets the general performance objective and requirements of § 73.20 and the performance capability requirements of § 73.45.

(b) *Security organization.* (1) The licensee shall establish a security organization, including guards. If a contract guard force is utilized for site security, the licensee's written agreement with the contractor 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 such reports and documents are kept by the licensee or the contractor, (iii) the requirement, in § 73.46(b)(4) of this section that the licensee demonstrate the ability of physical security personnel to perform their assigned duties and responsibilities, include demonstration of the ability of the contractor's physical security personnel to perform their assigned duties and responsibilities in carrying out the provisions of the Security Plan and these regulations, and (iv) the contractor will not assign any personnel to the site who have not first been made aware of these responsibilities.

(2) The licensee shall have onsite at all times at least one full time member of the security organization with authority to direct the physical protection activities of the security organization.

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

(ii) Provision for written approval of such procedures and any revisions thereto by the individual with overall responsibility for the security function.

(4) The licensee may not permit an individual to act as a Tactical Response Team member, armed response person, guard, or other member of the security organization unless the individual has been trained, equipped, and qualified to perform each assigned security duty in accordance with Appendix B of this part, ''General Criteria for Security Personnel.'' In addition, Tactical Response Team members, armed response personnel, and guards shall be trained, equipped, and qualified for use of their assigned weapons in accordance with paragraphs (b)(6) and (b)(7) of this section. Tactical Response Team members, armed response personnel, and guards shall also be trained and qualified in accordance with either paragraphs (b)(10) and (b)(11) or paragraph (b)(12) of this section. Upon the request of an authorized representative of the Commission, the licensee shall demonstrate the ability of the physical security personnel, whether licensee or contractor employees, to carry out their assigned duties and responsibilities. Each Tactical Response Team member, armed response person, and guard, whether a licensee or contractor employee, shall requalify in accordance with Appendix B of this part. Tactical Response Team members, armed response personnel, and guards shall also requalify in accordance with paragraph (b)(7) of this section at least once every 12 months. The licensee shall document the results of the qualification and requalification. The licensee shall retain the documentation of each qualification and requalification as a record for 3 years after each qualification and requalification.

(5) Within any given period of time, a member of the security organization may not be assigned to, or have direct

operational control over, more than one of the redundant elements of a physical protection subsystem if such assignment or control could result in the loss of effectiveness of the subsystem.

(6) Each guard shall be armed with a handgun, as described in appendix B of this part. Each Tactical Response Team member shall be armed with a 9mm semiautomatic pistol. All but one member of the Tactical Response Team shall be armed additionally with either a shotgun or semiautomatic rifle, as described in appendix B of this part. The remaining member of the Tactical Response Team shall carry, as an individually assigned weapon, a rifle of no less caliber than .30 inches or 7.62mm.

(7) In addition to the weapons qualification and requalification criteria of appendix B of this part, Tactical Response Team members, armed response personnel, and guards shall qualify and requalify, at least every 12 months, for day and night firing with assigned weapons in accordance with Appendix H of this part. Tactical Response Team members, armed response personnel, and guards shall be permitted to practice fire prior to qualification and requalification but shall be given only one opportunity to fire for record on the same calendar day. If a Tactical Response Team member, armed response person, or guard fails to qualify or requalify, the licensee shall remove the individual from security duties which require the use of firearms and retrain the individual prior to any subsequent attempt to qualify or requalify. If an individual fails to qualify or requalify on two successive attempts, he or she shall be required to receive additional training and successfully fire two consecutive qualifying scores prior to being reassigned to armed security duties.

(i) In addition, Tactical Response Team members, armed response personnel, and guards shall be prepared to demonstrate day and night firing qualification with their assigned weapons at any time upon request by an authorized representative of the NRC.

(ii) The licensee or the licensee's agent shall document the results of weapons qualification and requalification for day and night firing. The licensee shall retain the documentation of each qualification and requalification as a record for 3 years after each qualification and requalification.

(8) In addition to the training requirements contained in appendix B of this part, Tactical Response Team members shall successfully complete training in response tactics. The licensee shall document the completion of training. The licensee shall retain the documentation of training as a record for three years after training is completed.

(9) The licensee shall conduct Tactical Response Team and guard exercises to demonstrate the overall security system effectiveness and the ability of the security force to perform response and contingency plan responsibilities and to demonstrate individual skills in assigned team duties. During the first 12-month period following the date specified in paragraph (i)(2)(ii) of this section, an exercise must be carried out at least every three months for each shift, half of which are to be force-on-force. Subsequently, during each 12-month period commencing on the anniversary of the date specified in paragraph (i)(2)(ii) of this section, an exercise must be carried out at least every four months for each shift, one third of which are to be force-on-force. The licensee shall use these exercises to demonstrate its capability to respond to attempts to steal strategic special nuclear material. During each of the 12-month periods, the NRC shall observe one of the force-on-force exercises which demonstrates overall security system performance. The licensee shall notify the NRC of the scheduled exercise 60 days prior to that exercise. The licensee shall document the results of all exercises. The licensee shall retain the documentation of each exercise as a record for three years after each exercise is completed.

(10) In addition to the medical examinations and physical fitness requirements of paragraph I.C of Appendix B of this part, each Tactical Response Team member, armed response person, and guard, except as provided in paragraph (b)(10)(v) of this section, shall participate in a physical fitness training program on a continuing basis.

(i) The elements of the physical fitness training program must include, but not necessarily be limited to, the following:

(A) Training sessions of sufficient frequency, duration, and intensity to be of aerobic benefit, e.g., normally a frequency of three times per week, maintaining an intensity of approximately 75 percent of maximum heart rate for 20 minutes;

(B) Activities that use large muscle groups, that can be maintained continuously, and that are rhythmical and aerobic in nature, e.g., running, bicycling, rowing, swimming, or cross-country skiing; and

(C) Musculoskeletal training exercises that develop strength, flexibility, and endurance in the major muscle groups, e.g., legs, arms, and shoulders.

(ii) The licensee shall assess Tactical Response Team members, armed response personnel, and guards for general fitness once every 4 months to determine the effectiveness of the continuing physical fitness training program. Assessments must include a recent health history, measures of cardiovascular fitness, percent of body fat, flexibility, muscular strength, and endurance. Individual exercise programs must be modified to be consistent with the needs of each participating Tactical Response Team member, armed response person, and guard and consistent with the environments in which they must be prepared to perform their duties. Individuals who exceed 4 months without being assessed for general fitness due to excused time off from work must be assessed within 15 calendar days of returning to duty as a Tactical Response Team member, armed response person, or guard.

(iii) Within 30 days prior to participation in the physical fitness training program, the licensee shall give Tactical Response Team members, armed response personnel, and guards a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications, as disclosed by the medical examination, to participation in the physical fitness training program.

(iv) Licensees may temporarily waive an individual's participation in the physical fitness training program on the advice of the licensee's examining physician, during which time the individual may not be assigned duties as a Tactical Response Team member.

(v) Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the physical fitness training program specified in paragraph (b)(10) of this section, provided that they are not assigned temporary response guard duties.

(11) In addition to the physical fitness demonstration contained in paragraph I.C of Appendix B of this part, Tactical Response Team members, armed response personnel, and guards shall meet or exceed the requirements in paragraphs (b)(11)(i) through (b)(11)(v) of this section, except as provided in paragraph (b)(11)(vi) of this section, initially and at least once every 12 months thereafter.

(i) For Tactical Response Team members the criteria are a 1-mile run in 8 minutes and 30 seconds or less and a 40-yard dash starting from a prone position in 8 seconds or less. For armed response personnel and guards that are not members of the Tactical Response Team the criteria are a one-half mile run in 4 minutes and 40 seconds or less and a 40-yard dash starting from a prone position in 8.5 seconds or less. The test may be taken in ordinary athletic attire under the supervision of licensee designated personnel. The licensee shall retain a record of each individual's performance for 3 years.

(ii) Incumbent Tactical Response Team members, armed response personnel, and guards shall meet or exceed the qualification criteria within 12 months of NRC approval of the licensee's revised Fixed Site Physical Protection Plan. New employees hired after the approval date shall meet or exceed the qualification criteria prior to assignment as a Tactical Response Team member, armed response person, or guard.

(iii) Tactical Response Team members, armed response personnel, and guards shall be given a medical examination including a determination and

written certification by a licensed physician that there are no medical contraindications, as disclosed by the medical examination, to participation in the physical fitness performance testing. The medical examination must be given within 30 days prior to the first administration of the physical fitness performance test, and on an annual basis thereafter.

(iv) The licensee shall place Tactical Response Team members, armed response persons, and guards, who do not meet or exceed the qualification criteria, in a monitored remedial physical fitness training program and relieve them of security duties until they satisfactorily meet or exceed the qualification criteria.

(v) Licensees may temporarily waive the annual performance testing for an individual on the advice of the licensee's examining physician, during which time the individual may not be assigned duties as a Tactical Response Team member.

(vi) Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the annual performance testing specified in paragraph (b)(11) of this section, provided that they are not assigned temporary response guard duties.

(12) The licensee may elect to comply with the requirements of this paragraph instead of the requirements of paragraphs (b)(10) and (b)(11) of this section. In addition to the physical fitness qualifications of paragraph I.C of Appendix B of this part, each licensee subject to the requirements of this section shall develop and submit to the NRC for approval site specific, content-based, physical fitness performance tests which will—when administered to each Tactical Response Team member, armed response person, or guard—duplicate the response duties these individuals may need to perform during a strenuous tactical engagement.

(i) The test must be administered to each Tactical Response Team member, armed response person, and guard once every 3 months. The test must specifically address the physical capabilities needed by armed response personnel during a strenuous tactical engagement at the licensed facility. Individuals who exceed 3 months without having been administered the test due to excused time off from work must be tested within 15 calendar days of returning to duty as a Tactical Response Team member, armed response person, or guard.

(ii) Within 30 days before the first administration of the physical fitness performance test, and on an annual basis thereafter, Tactical Response Team members, armed response personnel, and guards shall be given a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications, as disclosed by the medical examination, to participation in the physical fitness performance test.

(iii) Guards whose duties are to staff the central or secondary alarm station and those who control exit or entry portals are exempt from the performance test specified in paragraph (b)(12) of this section, provided that they are not assigned temporary response guard duties.

(c) *Physical barrier subsystems.* (1) vital equipment must be located only within a vital area, and strategic special nuclear material must be stored or processed only in a material access area. Both vital areas and material access areas must be located within a protected area so that access to vital equipment and to strategic special nuclear material requires passage through at least three physical barriers. The perimeter of the protected area must be provided with two separated physical barriers with an intrusion detection system placed between the two. The inner barrier must be positioned and constructed to enhance assessment of penetration attempts and to delay attempts at unauthorized exit from the protected area. The perimeter of the protected area must also incorporate features and structures that prevent forcible vehicle entry. More than one vital area or material access 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 or material access 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 large enough 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.

(4) 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), (e)(8), (h)(4) and (h)(6) of this section, but not less than 0.2 footcandle measured horizontally at ground level.

(5) Strategic special nuclear material, other than alloys, fuel elements or fuel assemblies, shall:

(i) Be stored in a vault when not undergoing processing if the material can be used directly in the manufacture of a nuclear explosive device. Vaults used to protect such material shall be capable of preventing entry to stored SSNM by a single action in a forced entry attempt, except as such single action would both destroy the barrier and render contained SSNM incapable of being removed, and shall provide sufficient delay to prevent removal of stored SSNM prior to arrival of response personnel capable of neutralizing the design basis threat stated in §73.1.

(ii) Be stored in tamper-indicating containers;

(iii) Be processed only in material access areas constructed with barriers that provide significant delay to penetration; and

(iv) Be kept in locked compartments or locked process equipment while undergoing processing except when personally attended.

(6) Enriched uranium scrap (enriched to 20% or greater) in the form of small pieces, cuttings, chips, solutions or in other forms which result from a manufacturing process, contained in 30 gallon or larger containers with a uranium-235 content of less than 0.25 grams per liter, may be stored within a locked and separately fenced area within a larger protected area provided that the storage area fence is no closer than 25 feet to the perimeter of the protected area. The storage area when unoccupied shall be protected by a guard or watchman who shall patrol at intervals not exceeding 4 hours, or by intrusion alarms.

(d) *Access control subsystems and procedures.* (1) A numbered picture badge identification subsystem shall 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, material access, or vital areas may be authorized access to such areas without escort provided that he receives a picture badge upon entrance into the protected area and returns the badge upon exit from the protected area, and that the badge indicates, (i) Non-employee—no escort required; (ii) areas to which access is authorized and (iii) the period for which access has been authorized. Badges shall be displayed by all individuals while inside the protected areas.

(2) Unescorted access to vital areas, material access areas and controlled access areas shall be limited to individuals who are authorized access to the material and equipment in such areas, and who require such access to perform their duties. Access to material access areas shall include at least two individuals. Authorization for such individuals shall be indicated by the issuance of specially coded numbered badges indicating vital areas, material access areas, and controlled access areas to which access is authorized. No activities other than those which require access to strategic special nuclear material or to equipment used in the processing, use, or storage of strategic special nuclear material, or necessary maintenance, shall be permitted within a material access area.

(3) The licensee shall establish and follow written procedures that will permit access control personnel to identify those vehicles that are authorized and those materials that are not authorized entry to protected, material access, and vital areas. The licensee

shall retain 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 procedures is superseded, retain the superseded material for three years after each change.

(4)(i) The licensee shall control all points of personnel and vehicle access into a protected area. Identification and search of all individuals for firearms, explosives, and incendiary devices must be made and authorization must be checked at these points except for Federal, State, and local law enforcement personnel on official duty and United States Department of Energy couriers engaged in the transport of special nuclear material. The search function for detection of firearms, explosives, and incendiary devices must be accomplished through the use of detection equipment capable of detecting both firearms and explosives. The individual responsible for the last access control function (controlling admission to the protected area) shall be isolated within a structure with bullet resisting walls, doors, ceiling, floor, and windows.

(ii) When the licensee has cause to suspect that an individual is attempting to introduce firearms, explosives, or incendiary devices into a protected area, 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 search using the equipment.

(5) At the point of personnel and vehicle access into a protected area, all hand-carried packages except those carried by individuals exempted from personal search under the provisions of paragraph (d)(4)(i) of this part must be searched for firearms, explosives, and incendiary devices.

(6) All packages and material for delivery into a protected area must be checked for proper identification and authorization and searched for firearms, explosives, and incendiary devices 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 material access, vital, or protected areas for reasons of safety, security, or operational necessity.

(7) All vehicles, except United States Department of Energy vehicles engaged in transporting special nuclear material and emergency vehicles under emergency conditions, shall be searched for firearms, explosives, and incendiary devices prior to entry into the protected area. Vehicle areas to be searched shall include the cab, engine compartment, undercarriage, and cargo area.

(8) All vehicles, except designated licensee vehicles, requiring entry into the protected area shall be escorted by a member of the security organization while within the protected area, and to the extent practicable shall be off-loaded in an area that is not adjacent to a vital area. Designated licensee vehicles shall be limited in their use to onsite plant functions and shall remain in the protected area except for operational, maintenance, 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.

(9) The licensee shall control all points of personnel and vehicle access to material access areas, vital areas, and controlled access areas. At least two armed guards trained in accordance with the provisions contained in paragraph (b)(7) of this section and appendix B of this part shall be posted at each material access area control point whenever in use. Identification and authorization of personnel and vehicles must be verified at the material access area control point. Prior to entry into a material access area, packages must be searched for firearms, explosives, and incendiary devices. All vehicles, materials and packages, including trash, wastes, tools, and equipment exiting from a material access area must be searched for concealed strategic special nuclear material by a team of at least two individuals who are not authorized access to that material access area. Each individual exiting a material access area shall undergo at least two separate searches for

concealed strategic special nuclear material. For individuals exiting an area that contains only alloyed or encapsulated strategic special nuclear material, the second search may be conducted in a random manner.

(10) Before exiting from a material access area, containers of contaminated wastes must be drum scanned and tamper sealed by at least two individuals, working and recording their findings as a team, who do not have access to material processing and storage areas. The licensee shall retain the records of these findings for three years after the record is made.

(11) Strategic special nuclear material being prepared for shipment offsite, including product, samples and scrap, shall be packed and placed in sealed containers in the presence of at least two individuals working as a team who shall verify and certify the content of each shipping container through the witnessing of gross weight measurements and nondestructive assay, and through the inspection of tamper seal integrity and associated seal records.

(12) Areas used for preparing strategic special nuclear material for shipment and areas used for packaging and screening trash and wastes shall be controlled access areas and shall be separated from processing and storage areas.

(13) Individuals not permitted by the licensee to enter protected areas without escort must be escorted by a watchman or other individual designated by the licensee while in a protected area and must be badged to indicate that an escort is required. In addition, the individual shall be required to register his or her name, date, time, purpose of visit and employment affiliation, citizenship, and name of the individual to be visited in a log. The licensee shall retain each log as a record for three years after the last entry is made in the log.

(14) All keys, locks, combinations and related equipment used to control access to protected, material access, vital, and controlled access areas shall be controlled to reduce the probability of compromise. Whenever there is evidence that a key, lock, combination, or related equipment may have been compromised it shall be changed. Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access, shall be changed.

(15) The licensee may not announce or otherwise communicate to its employees or site contractors the arrival or presence of an NRC safeguards inspector unless specifically requested to do so by the NRC safeguards inspector.

(e) *Detection, surveillance and alarm subsystems and procedures.* (1) The licensee shall provide an intrusion alarm subsystem with a capability to detect penetration through the isolation zone and to permit response action.

(2) All emergency exits in each protected, material access, and vital area shall be locked to prevent entry from the outside and alarmed to provide local visible and audible alarm annunciation.

(3) All unoccupied vital areas and material access areas shall be locked and protected by an intrusion alarm subsystem which will alarm upon the entry of a person anywhere into the area, upon exit from the area, and upon movement of an individual within the area, except that for process material access areas only the location of the strategic special nuclear material within the area is required to be so alarmed. Vaults and process areas that contain strategic special nuclear material that has not been alloyed or encapsulated shall also be under the surveillance of closed circuit television that is monitored in both alarm stations. Additionally, means shall be employed which require that an individual other than an alarm station operator be present at or have knowledge of access to such unoccupied vaults or process areas.

(4) All manned access control points in the protected area barrier, all security patrols and guard stations within the protected area, and both alarm stations shall be provided with duress alarms.

(5) All alarms required pursuant to this section shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other independent continuously manned onsite station not necessarily within the protected

area, so that a single act cannot remove the capability of calling for assistance or responding to an alarm. The alarm stations shall be controlled access areas and their walls, doors, ceiling, floor, and windows shall be bullet-resisting. The central alarm station shall be located within a building so that the interior of the central alarm station is not visible from the perimeter of the protected area. This station may not contain any operational activities that would interfere with the execution of the alarm response function.

(6) All alarms required by this section shall remain operable from independent power sources in the event of the loss of normal power. Switchover to standby power shall be automatic and shall not cause false alarms on annunciator modules.

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

(8) All exterior areas within the protected area shall be monitored or periodically checked to detect the presence of unauthorized persons, vehicles, materials, or unauthorized activities.

(9) Methods to observe individuals within material access areas to assure that strategic special nuclear material is not moved to unauthorized locations or in an unauthorized manner shall be provided and used on a continuing basis.

(f) *Communication subsystems.* (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)(5) of this section, who shall be capable of calling for assistance from other guards, watchmen, and armed response personnel and from law enforcement authorities.

(2) Each alarm station required by paragraph (e)(5) of this section shall have both conventional telephone service and radio or microwave transmitted two-way voice communication, either directly or through an intermediary, for the capability of communication with the law enforcement authorities.

(3) 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) *Test and maintenance programs.* The licensee shall have a test and maintenance program for intrusion alarms, emergency exit alarms, communications equipment, physical barriers, and other physical protection related devices and equipment used pursuant to this section that shall provide for the following:

(1) Tests and inspections during the installation and construction of physical protection related subsystems and components to assure that they comply with their respective design criteria and performance specifications.

(2) Preoperational tests and inspections of physical protection related subsystems and components to demonstrate their effectiveness and availability with respect to their respective design criteria and performance specifications.

(3) Operational tests and inspections of physical protection related subsystems and components to assure their maintenance in an operable and effective condition, including:

(i) Testing of each intrusion alarm at the beginning and end of any period that it is used. If the period of continuous use is longer than seven days, the intrusion alarm shall also be tested at least once every seven days.

(ii) Testing of communications equipment required for communications onsite, including duress alarms, 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) Preventive maintenance programs shall be established for physical protection related subsystems and components to assure their continued maintenance in an operable and effective condition.

(5) All physical protection related subsystems and components shall be maintained in operable condition. The licensee shall develop and employ corrective action procedures and compensatory measures to assure that the effectiveness of the physical protection system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures. Repairs and maintenance shall be performed by at least two individuals working as a team who have been trained in the operation and performance of the equipment. The security organization shall be notified before and after service is performed and shall conduct performance verification tests after the service has been completed.

(6) The security program must be reviewed at least every 12 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program. 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, and any actions taken, must be documented in a report to the licensee's plant manager and to corporate management at least one level higher than that having responsibility for the day-to-day plant operations. These reports must be maintained in an auditable form, available for inspection for a period of 3 years.

(h) *Contingency and response plans and procedures.* (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 strategic special nuclear material and 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.'' Contingency plans must include, but not limited to, the response requirements listed in paragraphs (h)(2) through (h)(5) of this section. The licensee shall retain the current safeguards contingency plan as a record until the Commission terminates the license and, if any portion of the plan is superseded, retain that superseded portion for 3 years after the effective date of change.

(2) The licensee shall establish and document response arrangements that have been made with local law enforcement authorities. The licensee shall retain documentation of the current arrangements as a record until the Commission terminates each license requiring the arrangements and, if any arrangement is superseded, retain the superseded material for three years after each change.

(3) A Tactical Response Team consisting of a minimum of five (5) members must be available at the facility to fulfill assessment and response requirements. In addition, a force of guards or armed response personnel also must be available to provide assistance as necessary. The size and availability of the additional force must be determined on the basis of site-specific considerations that could affect the ability of the total onsite response force to engage and impede the adversary force until offsite assistance arrives. The rationale for the total number and availabiliy of onsite armed response personnel must be included in the physical protection plans submitted to the Commission for approval.

(4) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, a 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 purposes of radiological sabotage or theft of strategic 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 acts of radiological sabotage or theft of strategic special nuclear material 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 that 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.

(7) Alarms occurring within unoccupied vaults and unoccupied material access areas containing unalloyed or unencapsulated strategic special nuclear material shall be assessed by at least two security personnel using closed circuit television (CCTV) or other remote means.

(8) Alarms occurring within unoccupied material access areas that contain only alloyed or encapsulated strategic special nuclear material shall be assessed as in paragraph (h)(7) of this section or by at least two security personnel who shall undergo a search before exiting the material access area.

(i) *Implementation schedule for revisions to physical protection plans.* (1) By November 28, 1994, each licensee shall submit a revised Fixed Site Physical Protection Plan to the NRC for approval. The revised plan must describe how the licensee will comply with the requirements of paragraphs (b)(10) and (b)(11) of this section or the requirements of (b)(12) of this section. Revised plans must be mailed to the Director, Division of Fuel Management, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

(2) Each licensee shall implement the approved plan pursuant to paragraphs (b)(10) and (b)(11) of this section or (b)(12) of this section within 1 year after NRC approval of the revised Fixed Site Physical Protection Plan.

[44 FR 68194, Nov. 28, 1979, as amended at 53 FR 19258, May 27, 1988; 53 FR 23383, June 22, 1988; 53 FR 45452, Nov. 10, 1988; 57 FR 33430, July 29, 1992; 58 FR 29522, May 21, 1993; 58 FR 45784, Aug. 31, 1993; 59 FR 38348, July 28, 1994; 79 FR 75741, Dec. 19, 2014; 84 FR 65646, Nov. 29, 2019]

§ 73.50 Requirements for physical protection of licensed activities.

Each licensee who is not subject to § 73.51, but who possesses, uses, or stores formula quantities of strategic special nuclear material that are not readily separable from other radioactive material and which have a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surfaces without intervening shielding other than at a nuclear reactor facility licensed under parts 50 or 52 of this chapter, shall comply with the following:

(a) *Physical security organization.* (1) The licensee shall establish a security organization, including guards, to protect his facility against radiological sabotage and the special nuclear material in his possession against theft.

(2) At least one supervisor of the security organization shall be on site at all times.

(3) The licensee shall establish, maintain, and follow 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 retain 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 procedures is superseded, retain the superseded material for three years after each change.

(4) 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.

(b) *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. More than one vital area may be within a single protected area.

(2) The licensee shall locate material access areas only within protected areas such that access to the material access area requires passage through at least two physical barriers. More than one material access area may be within a single protected area.

(3) The physical barrier at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier within the protected area, and the intervening space monitored or periodically checked to detect the presence of persons or vehicles so that the facility security organization can respond to suspicious activity or to the breaching of any physical barrier.

(4) An isolation zone shall be maintained around the physical barrier at the perimeter of the protected area and any part of a building used as part of that physical barrier. The isolation zone shall be monitored to detect the presence of individuals or vehicles within the zone so as to allow response by armed members of the license security organization to be initiated at the time of penetration of the protected area. Parking facilities, both for employees and visitors, shall be located outside the isolation zone.

(5) Isolation zones and clear areas between barriers shall be provided with illumination sufficient for the monitoring required by paragraphs (b) (3) and (4) of this section, but not less than 0.2 foot candles.

(c) *Access requirements.* The licensee shall control all points of personnel and vehicle access into a protected area, including shipping or receiving areas, and into each vital area. Identification of personnel and vehicles shall be made and authorization shall be checked at such points.

(1) At the point of personnel and vehicle access into a protected area, all individuals, except employees who possess a NRC or United States Department of Energy access authorization, and 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. The search shall be conducted either by a physical search or by the use of equipment capable of detecting such devices. Employees who possess an NRC or Department of Energy access authorization shall be searched at random intervals. Subsequent to search, drivers of delivery and service vehicles shall be escorted at all times while within the protection area.

(2) All packages being delivered into the protected area shall be checked for proper identification and authorization. Packages other than hand-carried packages shall be searched at random intervals.

(3) A picture badge identification system shall be used for all individuals who are authorized access to protected areas without escort.

(4) Access to vital areas and material access areas shall be limited to individuals who are authorized access to vital equipment or special nuclear material and who require such access to perform their duties. Authorization for such individuals shall be provided by the issuance of specially coded numbered badges indicating vital areas and material access areas to which access is authorized. Unoccupied vital areas and

material access areas shall be protected by an active intrusion alarm system.

(5) Individuals not employed by the licensee must be escorted by a watchman, or other individual designated by the licensee, while in a protected area and must be badged to indicate that an escort is required. In addition, the licensee shall require that each individual not employed by the licensee register his or her name, date, time, purpose of visit, employment affiliation, citizenship, name and badge number of the escort, and name of the individual to be visited. The licensee shall retain the register of information for three years after the last entry is made in the register. Except for a driver of a delivery or service vehicle, an individual not employed by the licensee who requires frequent and extended access to a protected area or a vital area need not be escorted if the individual is provided with a picture badge, which the individual must receive upon entrance into the protected area and return each time he or she leaves the protected area, that indicates—

(i) Nonemployee-no escort required,

(ii) Areas to which access is authorized, and

(iii) The period for which access has been authorized.

(6) No vehicles used primarily for the conveyance of individuals shall be permitted within a protected area except under emergency conditions.

(7) Keys, locks, combinations, and related equipment shall be controlled to minimize the possibility of compromise and promptly changed whenever there is evidence that they have been compromised. Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access shall be changed.

(d) *Detection aids.* (1) All alarms required pursuant to this part shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station, not necessarily within the protected area, such that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm. All alarms shall be self-checking and tamper indicating. The annunciation of an alarm at the onsite central alarm station shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location. All intrusion alarms, emergency exit alarms, alarm systems, and line supervisory systems shall at minimum meet the performance and reliability levels indicated by GSA Interim Federal Specification W-A–00450 B (GSA-FSS). The GSA Interim Federal Specification has been approved for incorporation by reference by the Director of the Federal Register. A copy of the material is available for inspection at the NRC Library, 11545 Rockville Pike, Rockville, Maryland 20852-2738.

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

(e) *Communication requirements.* (1) Each guard or watchman on duty shall be capable of maintaining continuous communication with an individual in a continuously manned central alarm station within the protected area, who shall be capable of calling for assistance from other guards and watchmen and from local law enforcement authorities.

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

(3) To provide the capability of continuous communication, two-way radio voice communication shall be established in addition to conventional telephone service between local law enforcement authorities and the facility and shall terminate at the facility in a continuously manned central alarm station within the protected area.

(4) All communications equipment, including offsite equipment, shall remain operable from independent power sources in the event of loss of primary power.

(f) *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, communications equipment, physical barriers, and other security related devices or equipment shall be maintained in operable and effective condition.

(2) Each intrusion alarm shall be functionally tested for operability and required performance at the beginning and end of each interval during which it is used for security, but not less frequently than once every seven (7) days.

(3) Communications equipment shall be tested for operability and performance not less frequently than once at the beginning of each security personnel work shift.

(g) *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 special nuclear material and 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.'' The licensee shall retain the current safeguards contingency plan as a record until the Commission terminates the license and, if any portion of the plan is superseded, retain the superseded portion for 3 years after the effective date of the change.

(2) The licensee shall establish and document liaison with law enforcement authorities. The licensee shall retain the 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) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, a material access area, or a vital area; or upon evidence or indication of intrusion into a protected area, material access area, or vital area, the licensee security organization shall:

(i) Determine whether or not a threat exists,

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

(iii) Take immediate concurrent measures to neutralize the threat, by:

(A) Requiring responding guards to interpose themselves between material access areas and vital areas and any adversary attempting entry for the purpose of theft of special nuclear material or radiological sabotage and to intercept any person exiting with special nuclear material, and,

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

(4) The licensee shall instruct every guard to prevent or impede attempted acts of theft or radiological sabotage by using force sufficient to counter the force directed at him including deadly force when the guard has a reasonable belief it is necessary in self-defense or in the defense of others.

(h) 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 paragraph (a)(4) of this section.

(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, 5844))

[38 FR 35430, Dec. 28, 1973, as amended at 42 FR 64103, Dec. 22, 1977; 43 FR 11965, Mar. 23, 1978; 43 FR 37426, Aug. 23, 1978; 44 FR 68198, Nov. 28, 1979; 53 FR 19259, May 27, 1988; 57 FR 33430, July 29, 1992; 57 FR 61787, Dec. 29, 1992; 59 FR 50689, Oct. 5, 1994; 63 FR 26962, May 15, 1998; 72 FR 49561, Aug. 28, 2007; 86 FR 43403, Aug. 9, 2021; 88 FR 57879, Aug. 24, 2023]

§ 73.51 Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste.

(a) *Applicability.* Notwithstanding the provisions of §§ 73.20, 73.50, or 73.67, the physical protection requirements of this section apply to each licensee that stores spent nuclear fuel and high-level radioactive waste pursuant to paragraphs (a)(1)(i), (ii), and (2) of this section. This includes—

(1) Spent nuclear fuel and high-level radioactive waste stored under a specific license issued pursuant to part 72 of this chapter:

(i) At an independent spent fuel storage installation (ISFSI) or

(ii) At a monitored retrievable storage (MRS) installation; or

(2) Spent nuclear fuel and high-level radioactive waste at a geologic repository operations area (GROA) licensed pursuant to part 60 or 63 of this chapter;

(b) *General performance objectives.* (1) Each licensee subject to this section shall establish and maintain a physical protection system with the objective of providing high assurance that activities involving spent nuclear fuel and high-level radioactive waste do not constitute an unreasonable risk to public health and safety.

(2) To meet the general objective of paragraph (b)(1) of this section, each licensee subject to this section shall meet the following performance capabilities.

(i) Store spent nuclear fuel and high-level radioactive waste only within a protected area;

(ii) Grant access to the protected area only to individuals who are authorized to enter the protected area;

(iii) Detect and assess unauthorized penetration of, or activities within, the protected area;

(iv) Provide timely communication to a designated response force whenever necessary; and

(v) Manage the physical protection organization in a manner that maintains its effectiveness.

(3) The physical protection system must be designed to protect against loss of control of the facility that could be sufficient to cause a radiation exposure exceeding the dose as described in § 72.106 of this chapter.

(4)(i) The licensee must ensure that the firearms background check requirements of § 73.17 of this part are met for all members of the security organization whose official duties require access to covered weapons or who inventory enhanced weapons.

(ii) The provisions of this paragraph are only applicable to licensees subject to this section who are also subject to the firearms background check provisions of § 73.17 of this part.

(c) *Plan retention.* Each licensee subject to this section shall retain a copy of the effective physical protection plan as a record for 3 years or until termination of the license for which procedures were developed.

(d) *Physical protection systems, components, and procedures.* A licensee shall comply with the following provisions as methods acceptable to NRC for meeting the performance capabilities of § 73.51(b)(2). The Commission may, on a specific basis and upon request or on its own initiative, authorize other alternative measures for the protection of spent fuel and high-level radioactive waste subject to the requirements of this section, if after evaluation of the specific alternative measures, it finds reasonable assurance of compliance with the performance capabilities of paragraph (b)(2) of this section.

(1) Spent nuclear fuel and high-level radioactive waste must be stored only within a protected area so that access to this material requires passage through or penetration of two physical barriers, one barrier at the perimeter of the protected area and one barrier offering substantial penetration resistance. The physical barrier at the perimeter of the protected area must be as defined in § 73.2. Isolation zones, typically 20 feet wide each, on both sides of this barrier, must be provided to facilitate assessment. The barrier offering substantial resistance to penetration may be provided by an approved storage cask or building walls such as those of a reactor or fuel storage building.

(2) Illumination must be sufficient to permit adequate assessment of unauthorized penetrations of or activities within the protected area.

(3) The perimeter of the protected area must be subject to continual surveillance and be protected by an active intrusion alarm system which is capable of detecting penetrations through the isolation zone and that is monitored in a continually staffed primary alarm station and in one additional continually staffed location. The primary alarm station must be located within the protected area; have bullet-resisting walls, doors, ceiling, and floor; and the interior of the station must not be visible from outside the protected area. A timely means for assessment of alarms must also be provided. Regarding alarm monitoring,

the redundant location need only provide a summary indication that an alarm has been generated.

(4) The protected area must be monitored by daily random patrols.

(5) A security organization with written procedures must be established. The security organization must include sufficient personnel per shift to provide for monitoring of detection systems and the conduct of surveillance, assessment, access control, and communications to assure adequate response. Members of the security organization must be trained, equipped, qualified, and requalified to perform assigned job duties in accordance with appendix B to part 73, sections I.A, (1) (a) and (b), B(1)(a), and the applicable portions of II.

(6) Documented liaison with a designated response force or local law enforcement agency (LLEA) must be established to permit timely response to unauthorized penetration or activities.

(7) A personnel identification system and a controlled lock system must be established and maintained to limit access to authorized individuals.

(8) Redundant communications capability must be provided between onsite security force members and designated response force or LLEA.

(9) All individuals, vehicles, and hand-carried packages entering the protected area must be checked for proper authorization and visually searched for explosives before entry.

(10) Written response procedures must be established and maintained for addressing unauthorized penetration of, or activities within, the protected area including Category 5, ''Procedures,'' of appendix C to part 73. The licensee shall retain a copy of response procedures as a record for 3 years or until termination of the license for which the procedures were developed. Copies of superseded material must be retained for 3 years after each change or until termination of the license.

(11) All detection systems and supporting subsystems must be tamper indicating with line supervision. These systems, as well as surveillance/assessment and illumination systems, must be maintained in operable condition. Timely compensatory measures must be taken after discovery of inoperability, to assure that the effectiveness of the of the security system is not reduced.

(12) The physical protection program must be reviewed once every 24 months by individuals independent of both physical protection program management and personnel who have direct responsibility for implementation of the physical protection program. The physical protection program review must include an evaluation of the effectiveness of the physical protection system and a verification of the liaison established with the designated response force or LLEA.

(13) The following documentation must be retained as a record for 3 years after the record is made or until termination of the license. Duplicate records to those required under §72.180 of part 72 and §73.1210 of this part need not be retained under the requirements of this section:

(i) A log of individuals granted access to the protected area;

(ii) Screening records of members of the security organization;

(iii) A log of all patrols;

(iv) A record of each alarm received, identifying the type of alarm, location, date and time when received, and disposition of the alarm; and

(v) The physical protection program review reports.

(e) *GROA exemption.* A licensee that operates a GROA is exempt from the requirements of this section for that GROA after permanent closure of the GROA.

(f) *Response requirements.* Licensees must train each armed member of the security organization with access to enhanced weapons on 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.

[63 FR 26962, May 15, 1998, as amended at 63 FR 49414, Sept. 16, 1998; 66 FR 55816, Nov. 2, 2001; 88 FR 15890, Mar. 14, 2023]

§ 73.54 Protection of digital computer and communication systems and networks.

By November 23, 2009 each licensee currently licensed to operate a nuclear power plant under part 50 of this chapter shall submit, as specified in § 50.4 and § 50.90 of this chapter, a cyber security plan that satisfies the requirements of this section for Commission review and approval. Each submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule. Current applicants for an operating license or combined license who have submitted their applications to the Commission prior to the effective date of this rule must amend their applications to include a cyber security plan consistent with this section.

(a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.

(1) The licensee shall protect digital computer and communication systems and networks associated with:

(i) Safety-related and important-to-safety functions;

(ii) Security functions;

(iii) Emergency preparedness functions, including offsite communications; and

(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

(2) The licensee shall protect the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would:

(i) Adversely impact the integrity or confidentiality of data and/or software;

(ii) Deny access to systems, services, and/or data; and

(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.

(4) Conduct cyber security event notifications in accordance with the provisions of § 73.77.

(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, as amended at 80 FR 67275, Nov. 2, 2015]

§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.

(12)(i) The licensee must ensure that the firearms background check requirements of § 73.17 of this part are met for all members of the security organization whose official duties require access to covered weapons or who inventory enhanced weapons.

(ii) The provisions of this paragraph are only applicable to licensees subject to this section that are also subject to the firearms background check provisions of § 73.17 of this part.

(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, section VI, to this part, ''Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties,'' 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, section II, to this part, ''Nuclear Power Plant 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, section VI, 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 physical 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, section VI, 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 the 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 threats 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 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 operations. These reports must be maintained in an auditable form and 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 components 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 §§ 73.1200 and 73.1205 of this part.

(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, as amended at 77 FR 39909, July 6, 2012; 88 FR 15891, Mar. 14, 2023]

Subpart G—Access Authorization and Access Control Requirements for the Physical Protection of Special Nuclear Material

SOURCE: 88 FR 15891, Mar. 14, 2023, unless otherwise noted.

§ 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 access and unescorted access authorization, respectively, or the contractors or vendors supporting the licensee or applicant shall inform the individual of his or her right to review information collected to assure its accuracy, and provide the individual with an opportunity to correct any inaccurate or incomplete information that is developed by licensees, applicants, or contractors or vendors about the individual.

(i) The subject individual may withdraw his or her consent at any time. Licensees, applicants, and contractors or vendors shall inform the individual that:

(A) Withdrawal of his or her consent will remove the individual's application for access authorization under the licensee's or applicant's access authorization program or contractor or vendor access authorization program; and

(B) Other licensees and applicants shall have access to information documenting the withdrawal. Additionally, the contractors or vendors may have the same access to the information, if such information is necessary for assisting licensees or applicants complying with requirements set forth in this section.

(ii) If an individual withdraws his or her consent, licensees, applicants, and contractors or vendors may not initiate any elements of the background investigation that were not in progress at the time the individual withdrew his or her consent, but shall complete any background investigation elements

that are in progress at the time consent is withdrawn. The licensee or applicant shall record the status of the individual's application for unescorted access or unescorted access authorization, respectively. Contractors or vendors may record the status of the individual's application for unescorted access or unescorted access authorization for licensees or applicants. Additionally, licensees, applicants, or contractors or vendors shall collect and maintain the individual's application for unescorted access or unescorted access authorization; his or her withdrawal of consent for the background investigation; the reason given by the individual for the withdrawal; and any pertinent information collected from the background investigation elements that were completed. This information must be shared with other licensees in accordance with paragraph (o)(6) of this section.

(iii) Licensees, applicants, and contractors or vendors shall inform, in writing, any individual who is applying for unescorted access or unescorted access authorization that the following actions are sufficient cause for denial or unfavorable termination of unescorted access or unescorted access authorization status:

(A) Refusal to provide a signed consent for the background investigation;

(B) Refusal to provide, or the falsification of, any personal history information required under this section, including the failure to report any previous denial or unfavorable termination of unescorted access or unescorted access authorization;

(C) Refusal to provide signed consent for the sharing of personal information with other licensees, applicants, or the contractor or vendors under paragraph (d)(4)(v) of this section; or

(D) Failure to report any arrests or legal actions specified in paragraph (g) of this section.

(2) *Personal history disclosure.* (i) Any individual who is applying for unescorted access or unescorted access authorization shall disclose the personal history information that is required by the licensee's or applicant's access authorization program, including any information that may be necessary for the reviewing official to make a determination of the individual's trustworthiness and reliability.

(ii) Licensees, applicants, and contractors or vendors shall not require an individual to disclose an administrative withdrawal of unescorted access or unescorted access authorization under the requirements of §73.56(g), (h)(7), or (i)(1)(v) of this section. However, the individual must disclose this information if the individual's unescorted access or unescorted access authorization is administratively withdrawn at the time he or she is seeking unescorted access or unescorted access authorization, or the individual's unescorted access or unescorted access authorization was subsequently denied or terminated unfavorably by a licensee, applicant, or contractor or vendor.

(3) *Verification of true identity.* Licensees, applicants, and contractors or vendors shall verify the true identity of an individual who is applying for unescorted access or unescorted access authorization in order to ensure that the applicant is the person that he or she has claimed to be. At a minimum, licensees, applicants, and contractors or vendors shall validate that the social security number that the individual has provided is his or hers, and, in the case of foreign nationals, validate the claimed non-immigration status that the individual has provided is correct. In addition, licensees and applicants shall also determine whether the results of the fingerprinting required under §73.57 confirm the individual's claimed identity, if such results are available.

(4) *Employment history evaluation.* Licensees, applicants, and contractors or vendors shall ensure that an employment history evaluation has been completed on a best effort basis, by questioning the individual's present and former employers, and by determining the activities of the individual while unemployed.

(i) For the claimed employment period, the individual must provide the reason for any termination, eligibility for rehire, and other information that could reflect on the individual's trustworthiness and reliability.

(ii) If the claimed employment was military service the individual shall provide a characterization of service,

reason for separation, and any disciplinary actions that could affect a trustworthiness and reliability determination.

(iii) If education is claimed in lieu of employment, the individual shall provide any information related to the claimed education that could reflect on the individual's trustworthiness and reliability and, at a minimum, verify that the individual was registered for the classes and received grades that indicate that the individual participated in the educational process during the claimed period.

(iv) If a previous employer, educational institution, or any other entity with which the individual claims to have been engaged fails to provide information or indicates an inability or unwillingness to provide information within 3 business days of the request, the licensee, applicant, or contractor or vendor shall:

(A) Document this refusal or unwillingness in the licensee's, applicant's, or contractor's or vendor's record of the investigation; and

(B) Obtain a confirmation of employment, educational enrollment and attendance, or other form of engagement claimed by the individual from at least one alternate source that has not been previously used.

(v) When any licensee, applicant, contractor, or vendor is seeking the information required for an unescorted access or unescorted access authorization decision under this section and has obtained a signed release from the subject individual authorizing the disclosure of such information, other licensees, applicants, contractors and vendors shall make available the personal or access authorization information requested regarding the denial or unfavorable termination of unescorted access or unescorted access authorization.

(vi) In conducting an employment history evaluation, the licensee, applicant, contractor, or vendor may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or e-mail. Licensees, applicants, contractors, or vendors shall make a record of the contents of the telephone call and shall retain that record, and any documents or electronic files obtained electronically, in accordance with paragraph (o) of this section.

(5) *Credit history evaluation.* Licensees, applicants, contractors and vendors shall ensure that the full credit history of any individual who is applying for unescorted access or unescorted access authorization is evaluated. A full credit history evaluation must include, but is not limited to, an inquiry to detect potential fraud or misuse of social security numbers or other financial identifiers, and a review and evaluation of all of the information that is provided by a national credit-reporting agency about the individual's credit history. For individuals including foreign nationals and United States citizens who have resided outside the United States and do not have established credit history that covers at least the most recent seven years in the United States, the licensee, applicant, contractor or vendor must document all attempts to obtain information regarding the individual's credit history and financial responsibility from some relevant entity located in that other country or countries.

(6) *Character and reputation evaluation.* Licensees, applicants, contractors, and vendors shall ascertain the character and reputation of an individual who has applied for unescorted access or unescorted access authorization by conducting reference checks. Reference checks may not be conducted with any person who is known to be a close member of the individual's family, including but not limited to, the individual's spouse, parents, siblings, or children, or any individual who resides in the individual's permanent household. The reference checks must focus on the individual's reputation for trustworthiness and reliability.

(7) *Criminal history review.* The licensee's or applicant's reviewing official shall evaluate the entire criminal history record of an individual who is applying for unescorted access or unescorted access authorization to determine whether the individual has a record of criminal activity that may adversely impact his or her trustworthiness and reliability. A criminal history record must be obtained in accordance with the requirements of

§ 73.57. For individuals who do not have or are not expected to have unescorted access, a criminal history record of the individual shall be obtained in accordance with the requirements set forth in paragraph (k)(1)(ii) of this section.

(e) *Psychological assessment.* In order to assist in determining an individual's trustworthiness and reliability, licensees, applicants, contractors or vendors shall ensure that a psychological assessment has been completed before the individual is granted unescorted access or certified unescorted access authorization. Individuals who are applying for initial unescorted access or unescorted access authorization, or who have not maintained unescorted access or unescorted access authorization for greater than 365 days, shall be subject to a psychological assessment. The psychological assessment must be designed to evaluate the possible adverse impact of any noted psychological characteristics on the individual's trustworthiness and reliability.

(1) A licensed psychologist or psychiatrist with the appropriate training and experience shall conduct the psychological assessment.

(2) The psychological assessment must be conducted in accordance with the applicable ethical principles for conducting such assessments established by the American Psychological Association or American Psychiatric Association.

(3) At a minimum, the psychological assessment must include the administration and interpretation of a standardized, objective, professionally-accepted psychological test that provides information to identify indications of disturbances in personality or psychopathology that may have adverse implications for an individual's trustworthiness and reliability. A psychiatrist or psychologist specified in paragraph (e) of this section shall establish the predetermined thresholds for each scale, in accordance with paragraph (e)(2) of this section, that must be applied in interpreting the results of the psychological test to determine whether an individual must be interviewed by a licensed psychiatrist or psychologist, under § 73.56(e)(4)(i) of this section.

(4) The psychological assessment must include a clinical interview:

(i) If an individual's scores on the psychological test in paragraph (e)(3) of this section identify indications of disturbances in personality or psychopathology that may have implications for an individual's trustworthiness and reliability; or

(ii) If the individual is a member of the population that performs one or more job functions that are critical to the safe and secure operation of the licensee's facility, as defined in paragraph (i)(1)(v)(B) of this section.

(5) In the course of conducting a psychological assessment for those individuals who are specified in paragraph (h) of this section for initial unescorted access or unescorted access authorization category, if the licensed psychologist or psychiatrist identifies or discovers any information, including a medical condition, that could adversely impact the individual's fitness for duty or trustworthiness and reliability, the licensee, applicant, or contractor or vendor shall ensure that the psychologist or psychiatrist contact appropriate medical personnel to obtain further information as need for a determination. The results of the evaluation and a recommendation shall be provided to the licensee's or applicant's reviewing official.

(6) During psychological reassessments, if the licensed psychologist or psychiatrist identifies or discovers any information, including a medical condition, that could adversely impact the fitness for duty or trustworthiness and reliability of those individuals who are currently granted unescorted access or certified unescorted access authorization status, he or she shall inform (1) the reviewing official of the discovery within 24 hours of the discovery and (2) the medical personnel designated in the site implementing procedures, who shall ensure that an appropriate evaluation of the possible medical condition is conducted under the requirements of part 26 of this chapter. The results of the evaluation and a recommendation shall be provided to the licensee's or applicant's reviewing official.

(f) *Behavioral observation.* (1) Licensee and applicant access authorization programs must include a behavioral observation program that is designed to detect 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. Licensees, applicants and contractors or vendors must ensure that the individuals specified in paragraph (b)(1) and, if applicable, (b)(2) of this section are subject to behavioral observation.

(2) Each person subject to the behavior observation program shall be responsible for communicating to the licensee or applicant observed behaviors of individuals subject to the requirements of this section. Such behaviors include any behavior of individuals that may adversely affect the safety or security of the licensee's facility or that may constitute an unreasonable risk to the public health and safety or the common defense and security, including a potential threat to commit radiological sabotage.

(i) Licensees, applicants, and contractors or vendors shall ensure that individuals who are subject to this section also successfully complete initial behavioral observation training and requalification behavior observation training as required in paragraphs (f)(2)(ii) and (iii) of this section.

(ii) Behavioral observation training must be:

(A) Completed before the licensee grants unescorted access or certifies unescorted access authorization or an applicant certifies unescorted access authorization, as defined in paragraph (h)(4)(ii) of this section,

(B) Current before the licensee grants unescorted access update or reinstatement or licensee or applicant certifies unescorted access authorization reinstatement as defined in paragraph (h)(4)(ii) of this section, and

(C) Maintained in a current status during any period of time an individual possesses unescorted access or unescorted access authorization in accordance with paragraph (f)(2)(iv) of this section.

(iii) For initial behavioral observation training, individuals shall demonstrate completion by passing a comprehensive examination that addresses the knowledge and abilities necessary to detect behavior or activities that have the potential to 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. Remedial training and re-testing are required for individuals who fail to satisfactorily complete the examination.

(iv) Individuals shall complete refresher training on a nominal 12-month frequency, or more frequently where the need is indicated. Individuals may take and pass a comprehensive examination that meets the requirements of paragraph (f)(2)(iii) of this section in lieu of completing annual refresher training.

(v) Initial and refresher training may be delivered using a variety of media, including, but not limited to, classroom lectures, required reading, video, or computer-based training systems. The licensee, applicant, or contractor or vendor shall monitor the completion of training.

(3) Individuals who are subject to an access authorization program under this section shall at a minimum, report any concerns arising from behavioral observation, including, but not limited to, concerns related to any questionable behavior patterns or activities of others to the reviewing official, his or her supervisor, or other management personnel designated in their site procedures. The recipient of the report shall, if other than the reviewing official, promptly convey the report to the reviewing official, who shall reassess the reported individual's unescorted access or unescorted access authorization status. The reviewing official shall determine the elements of the reassessment based on the accumulated information of the individual. If the reviewing official has a reason to believe that the reported individual's trustworthiness or reliability is questionable, the reviewing official shall either administratively withdraw or terminate the individual's unescorted access or unescorted access authorization while completing the re-evaluation or investigation. If the reviewing official

determines from the information provided that there is cause for additional action, the reviewing official may inform the supervisor of the reported individual.

(g) *Self-reporting of legal actions.* (1) Any individual who has applied for unescorted access or unescorted access authorization or is maintaining unescorted access or unescorted access authorization under this section shall promptly report to the reviewing official, his or her supervisor, or other management personnel designated in site procedures any legal action(s) taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that requires a court appearance, including but not limited to an arrest, an indictment, the filing of charges, or a conviction, but excluding minor civil actions or misdemeanors such as parking violations or speeding tickets. The recipient of the report shall, if other than the reviewing official, promptly convey the report to the reviewing official. On the day that the report is received, the reviewing official shall evaluate the circumstances related to the reported legal action(s) and re-determine the reported individual's unescorted access or unescorted access authorization status.

(2) The licensee or applicant shall inform the individual of this obligation, in writing, prior to granting unescorted access or certifying unescorted access authorization.

(h) *Granting unescorted access and certifying unescorted access authorization.* Licensees and applicants shall implement the requirements of this paragraph for granting or certifying initial or reinstated unescorted access or unescorted access authorization. The investigatory information collected to satisfy the requirements of this section for individuals who are being considered for unescorted access or unescorted access authorization shall be valid for a trustworthiness and reliability determination by a licensee or applicant for 30 calendar days.

(1) *Determination basis.* (i) The licensee's or applicant's reviewing official shall determine whether to grant, certify, deny, unfavorably terminate, maintain, or administratively withdraw an individual's unescorted access or unescorted access authorization status, based on an evaluation of all of the information required by this section.

(ii) The licensee's or applicant's reviewing official may not grant unescorted access or certify unescorted access authorization status to an individual until all of the information required by this section has been evaluated by the reviewing official and the reviewing official has determined that the accumulated information supports a determination of the individual's trustworthiness and reliability. However, the reviewing official may deny or terminate unescorted access or unescorted access authorization of any individual based on disqualifying information even if not all the information required by this section has been collected or evaluated.

(2) *Unescorted access for NRC-certified personnel.* Licensees and applicants shall grant unescorted access to any individual who has been certified by the Nuclear Regulatory Commission as suitable for such access.

(3) *Access denial.* Licensees or applicants may not permit an individual, who is identified as having an access-denied status by another licensee subject to this section, or has an access authorization status other than favorably terminated, to enter any nuclear power plant protected area or vital area, under escort or otherwise, or take actions by electronic means that could adversely impact the licensee's or applicant's safety, security, or emergency response or their facilities, under supervision or otherwise, except upon completion of the initial unescorted access authorization process.

(4) *Granting unescorted access and certifying unescorted access authorization—* (i) *Initial unescorted access or unescorted access authorization.* In satisfying the requirements of paragraph (h)(1) of this section, for individuals who have never held unescorted access or unescorted access authorization status or whose unescorted access or unescorted access authorization status has been interrupted for a period of 3 years or more, the licensee, applicant, or contractor or vendor shall satisfy the requirements of paragraphs (d), (e), (f), and (g)

of this section. In meeting requirements set forth in paragraph (d)(4) of this section, the licensee, applicant, or contractor or vendor shall evaluate the 3 years before the date on which the application for unescorted access was submitted, or since the individual's eighteenth birthday, whichever is shorter. For the 1-year period preceding the date upon which the individual applies for unescorted access or unescorted access authorization, the licensee, applicant or contractor or vendor shall ensure that the employment history evaluation is conducted with every employer, regardless of the length of employment. For the remaining 2-year period, the licensee, applicant, or contractor or vendor shall ensure that the employment history evaluation is conducted with the employer by whom the individual claims to have been employed the longest within each calendar month.

(ii) *Interruption of unescorted access or unescorted access authorization.* In satisfying the requirements of paragraph (h)(1) of this section, for individuals who have previously been granted unescorted access or unescorted access authorization, but whose access had been terminated under favorable conditions, licensees, applicants or contractors or vendors shall satisfy the requirements of paragraphs (d), (e), (f), and (g) of this section, with consideration of the specific requirements for periods of interruption described below in paragraphs (h)(4)(ii)(A) or (h)(4)(ii)(B) of this section, as applicable. However, for individuals whose unescorted access or unescorted access authorization was interrupted for less than or equal to 30 calendar days, licensees, applicants, or contractors or vendors must only satisfy the requirements set forth in paragraphs (d)(1), (d)(2), and (d)(3) of this section. The applicable periods of interruption are determined by the number of calendar days between the day after the individual's access was terminated and the day upon which the individual applies for unescorted access or unescorted access authorization.

(A) *Update of unescorted access or unescorted access authorization.* For individuals whose last unescorted access or unescorted access authorization status has been interrupted for more than 30 calendar days but less than or equal to 365 calendar days, the licensee, applicant or contractor or vendor shall complete the individual's employment history evaluation in accordance with the requirements of paragraph (d)(4) of this section, within 5 business days after reinstatement. The licensee, applicant, or contractor or vendor shall ensure that the employment history evaluation has been conducted with the employer by whom the individual claims to have been employed the longest within the calendar month. However, if the employment history evaluation is not completed within 5 business days of reinstatement due to circumstances that are outside of the licensee's, applicant's, or contractor's or vendor's control and the licensee or applicant, contractor or vendor is not aware of any potentially disqualifying information regarding the individual within the past 5 years, the licensee may extend the individual's unescorted access an additional 5 business days. If the employment history evaluation is not completed within this extended 5 business days, the licensee shall administratively withdraw unescorted access and complete the employment history evaluation in accordance with § 73.56(d)(4) of this section. For re-certification of unescorted access authorization, prior to re-certification of unescorted access authorization status of an individual, the licensee or applicant shall complete all the elements stated above including drug screening and employment evaluation.

(B) *Reinstatement of unescorted access or unescorted access authorization.* For individuals whose last unescorted access or unescorted access authorization status has been interrupted for greater than 365 calendar days but fewer than 3 years the licensee, applicant or contractor or vendor shall evaluate the period of time since the individual last held unescorted access or unescorted access authorization status, up to and including the day the individual applies for re-instated unescorted access authorization. For the 1-year period preceding the date upon which the individual applies for unescorted access authorization, the licensee, applicant, or contractor or vendor shall ensure that

the employment history evaluation is conducted with every employer, regardless of the length of employment. For the remaining period, the licensee, applicant or contractor or vendor shall ensure that the employment history evaluation is conducted with the employer by whom the individual claims to have been employed the longest within each calendar month. In addition, the individual shall be subject to the psychological assessment required in § 73.56(e).

(5) *Accepting unescorted access authorization from other access authorization programs.* Licensees who are seeking to grant unescorted access or certify unescorted access authorization or applicants who are seeking to certify unescorted access authorization to an individual who is subject to another access authorization program or another access authorization program that complies with this section may rely on those access authorization programs or access authorization program elements to comply with the requirements of this section. However, the licensee who is seeking to grant unescorted access or the licensee or applicant who is seeking to certify unescorted access authorization shall ensure that the program elements to be accepted have been maintained consistent with the requirements of this section by the other access authorization program.

(6) *Information sharing.* To meet the requirements of this section, licensees, applicants, and contractors or vendors may rely upon the information that other licensees, applicants, and contractors or vendors who are also subject to this section, have gathered about individuals who have previously applied for unescorted access or unescorted access authorization, and developed about individuals during periods in which the individuals maintained unescorted access or unescorted access authorization status.

(i) Maintaining unescorted access or unescorted access authorization.

(1) Individuals may maintain unescorted access or unescorted access authorization status under the following conditions:

(i) The individual remains subject to a behavioral observation program that complies with the requirements of § 73.56(f) of this section.

(ii) The individual successfully completes behavioral observation refresher training or testing on the nominal 12-month frequency required in § 73.56(f)(2)(ii) of this section.

(iii) The individual complies with the licensee's or applicant's access authorization program policies and procedures to which he or she is subject, including the self-reporting of legal actions responsibility specified in paragraph (g) of this section.

(iv) The individual is subject to an annual (within 365 calendar days) supervisory review conducted in accordance with the requirements of the licensee's or applicant's behavioral observation program. The individual shall be subject to a supervisory interview in accordance with the requirements of the licensee's or applicant's behavioral observation program, if the supervisor does not have the frequent interaction with the individual throughout the review period needed to form an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability.

(v) The licensee's or applicant's reviewing official determines that the individual continues to be trustworthy and reliable. This determination must, at a minimum, be based on the following:

(A) A criminal history update and credit history re-evaluation for any individual with unescorted access. The criminal history update and credit history re-evaluation must be completed within 5 years of the date on which these elements were last completed.

(B) For individuals who perform one or more of the job functions described in this paragraph, the trustworthiness and reliability determination must be based on a criminal history update and credit history re-evaluation within three years of the date on which these elements were last completed, or more frequently, based on job assignment as determined by the licensee or applicant, and a psychological re-assessment within 5 years of the date on which this element was last completed:

(*1*) Individuals who have extensive knowledge of defensive strategies and

design and/or implementation of the plant's defense strategies, including—

(*i*) Site security supervisors;

(*ii*) Site security managers;

(*iii*) Security training instructors; and

(*iv*) Corporate security managers;

(*2*) Individuals in a position to grant an applicant unescorted access or unescorted access authorization, including site access authorization managers;

(*3*) Individuals assigned a duty to search for contraband or other items that could be used to commit radiological sabotage (*i.e.*, weapons, explosives, incendiary devices);

(*4*) Individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in §73.54, including—

(*i*) Plant network systems administrators;

(*ii*) IT personnel who are responsible for securing plant networks; or

(*5*) Individuals qualified for and assigned duties as: armed security officers, armed responders, alarm station operators, response team leaders, and armorers as defined in the licensee's or applicant's Physical Security Plan; and reactor operators, senior reactor operators and non-licensed operators. Non-licensed operators include those individuals responsible for the operation of plant systems and components, as directed by a reactor operator or senior reactor operator. A non-licensed operator also includes individuals who monitor plant instrumentation and equipment and principally perform their duties outside of the control room.

(C) The criminal history update and the credit history re-evaluation shall be completed within 30 calendar days of each other.

(vi) If the criminal history update, credit history re-evaluation, psychological re-assessment, if required, and supervisory review and interview, if applicable, have not been completed and the information evaluated by the reviewing official within the time frame specified under paragraph (v) of this section, the licensee or applicant shall administratively withdraw the individual's unescorted access or unescorted access authorization until these requirements have been met.

(2) If an individual who has unescorted access or unescorted access authorization status is not subject to an access authorization program that meets the requirements of this part for more than 30 continuous days, then the licensee or applicant shall terminate the individual's unescorted access or unescorted access authorization status and the individual shall meet the requirements in this section, as applicable, to regain unescorted access or unescorted access authorization.

(j) *Access to vital areas.* Licensees or applicants shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas during non-emergency conditions. The list must include only those individuals who have a continued need for access to those specific vital areas in order to perform their duties and responsibilities. The list must be approved by a cognizant licensee or applicant manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each vital area, and updated and re-approved no less frequently than every 31 days.

(k) *Trustworthiness and reliability of background screeners and access authorization program personnel.* Licensees, applicants, and contractors or vendors shall ensure that any individual who collects, processes, or has access to personal information that is used to make unescorted access or unescorted access authorization determinations under this section has been determined to be trustworthy and reliable.

(1) *Background screeners.* Licensees, applicants, and contractors or vendors who rely on individuals who are not directly under their control to collect and process information that will be used by a reviewing official to make unescorted access or unescorted access authorization determinations shall ensure that a trustworthiness and reliability evaluation of such individuals has been completed to support a determination that such individuals are

trustworthy and reliable. At a minimum, the following checks are required:

(i) Verify the individual's true identity as specified in paragraph (d)(3) of this section;

(ii) A local criminal history review and evaluation based on information obtained from an appropriate State or local court or agency in which the individual resided;

(iii) A credit history review and evaluation;

(iv) An employment history review and evaluation covering the past 3 years; and

(v) An evaluation of character and reputation.

(2) *Access authorization program personnel.* Licensees, applicants, and contractors or vendors shall ensure that any individual who evaluates personal information for the purpose of processing applications for unescorted access or unescorted access authorization, including but not limited to a psychologist or psychiatrist who conducts psychological assessments under §73.56(e), has access to the files, records, and personal information associated with individuals who have applied for unescorted access or unescorted access authorization, or is responsible for managing any databases that contain such files, records, and personal information has been determined to be trustworthy and reliable, as follows:

(i) The individual is subject to an access authorization program that meets the requirements of this section; or

(ii) The licensee, applicant, and contractor or vendor determines that the individual is trustworthy and reliable based upon an evaluation that meets the requirements of §73.56(d)(1) through (d)(6) and (e) and either a local criminal history review and evaluation as specified in §73.56(k)(1)(ii) or a criminal history check that meets the requirements of §73.56(d)(7).

(l) *Review procedures.* Each licensee and applicant shall include a procedure for the notification of individuals who are denied unescorted access, unescorted access authorization, or who are unfavorably terminated. Additionally, procedures must include provisions for the review, at the request of the affected individual, of a denial or unfavorable termination of unescorted access or unescorted access authorization that may adversely affect employment. The procedure must contain a provision to ensure the individual is informed of the grounds for the denial or unfavorable termination and allow the individual an opportunity to provide additional relevant information and an opportunity for an objective review of the information upon which the denial or unfavorable termination of unescorted access or unescorted access authorization was based. The procedure must provide for an impartial and independent internal management review. Licensees and applicants shall not grant unescorted access or certify unescorted access authorization, or permit the individual to maintain unescorted access or unescorted access authorization during the review process.

(m) *Protection of information.* Each licensee, applicant, contractor, or vendor shall establish and maintain a system of files and procedures to ensure personal information is not disclosed to unauthorized persons.

(1) Licensees, applicants and contractors or vendors shall obtain signed consent from the subject individual that authorizes the disclosure of any information collected and maintained under this section before disclosing the information, except for disclosures to the following individuals:

(i) The subject individual or his or her representative, when the individual has designated the representative in writing for specified unescorted access authorization matters;

(ii) NRC representatives;

(iii) Appropriate law enforcement officials under court order;

(iv) A licensee's, applicant's, or contractor's or vendor's representatives who have a need to have access to the information in performing assigned duties, including determinations of trustworthiness and reliability and audits of access authorization programs;

(v) The presiding officer in a judicial or administrative proceeding that is initiated by the subject individual;

(vi) Persons deciding matters under the review procedures in paragraph (k) of this section; or

(vii) Other persons pursuant to court order.

(2) All information pertaining to a denial or unfavorable termination of the individual's unescorted access or unescorted access authorization shall be promptly provided, upon receipt of a written request by the subject individual or his or her designated representative as designated in writing. The licensee or applicant may redact the information to be released to the extent that personal privacy information, including the name of the source of the information is withheld.

(3) A contract with any individual or organization who collects and maintains personal information that is relevant to an unescorted access or unescorted access authorization determination must require that such records be held in confidence, except as provided in paragraphs (m)(1) through (m)(2) of this section.

(4) Licensees, applicants, or contractors or vendors and any individual or organization who collects and maintains personal information on behalf of a licensee, applicant, or contractor or vendor, shall establish, implement, and maintain a system and procedures for the secure storage and handling of the information collected.

(n) *Audits and corrective action.* Each licensee and applicant shall be responsible for the continuing effectiveness of the access authorization program, including access authorization program elements that are provided by the contractors or vendors, and the access authorization programs of any of the contractors or vendors that are accepted by the licensee or applicant. Each licensee, applicant, and contractor or vendor shall ensure that access authorization programs and program elements are audited to confirm compliance with the requirements of this section and those comprehensive actions are taken to correct any non-conformance that is identified.

(1) Each licensee and applicant shall ensure that its entire access authorization program is audited nominally every 24 months. Licensees, applicants and contractors or vendors are responsible for determining the appropriate frequency, scope, and depth of additional auditing activities within the nominal 24-month period based on the review of program performance indicators, such as the frequency, nature, and severity of discovered problems, personnel or procedural changes, and previous audit findings.

(2) Access authorization program services that are provided to a licensee or applicant by contractor or vendor personnel who are off site or are not under the direct daily supervision or observation of the licensee's or applicant's personnel must be audited by the licensee or applicant on a nominal 12-month frequency. In addition, any access authorization program services that are provided to contractors or vendors by subcontractor personnel who are off site or are not under the direct daily supervision or observation of the contractor's or vendor's personnel must be audited by the licensee or applicant on a nominal 12-month frequency.

(3) Licensee's and applicant's contracts with contractors or vendors must reserve the licensee's or applicant's right to audit the contractors or vendors and the contractor's or vendor's subcontractors providing access authorization program services at any time, including at unannounced times, as well as to review all information and documentation that is reasonably relevant to the performance of the program.

(4) Licensee's and applicant's contracts with the contractors or vendors, and contractors' or vendors' contracts with subcontractors, must also require that the licensee or applicant shall be provided access to and be permitted to take away copies of any documents or data that may be needed to assure that the contractor or vendor and its subcontractors are performing their functions properly and that staff and procedures meet applicable requirements.

(5) Audits must focus on the effectiveness of the access authorization program or program element(s), as appropriate. At least one member of the licensee or applicant audit team shall be a person who is knowledgeable of and practiced with meeting the performance objectives and requirements of the access authorization program or program elements being audited. The individuals performing the audit of the

access authorization program or program element(s) shall be independent from both the subject access authorization programs' management and from personnel who are directly responsible for implementing the access authorization program or program elements being audited.

(6) The results of the audits, along with any recommendations, must be documented in the site corrective action program in accordance with §73.55(b)(10) and reported to senior management having responsibility in the area audited and to management responsible for the access authorization program. Each audit report must identify conditions that are adverse to the proper performance of the access authorization program, the cause of the condition(s), and, when appropriate, recommended corrective actions, and corrective actions taken. The licensee, applicant, or contractor or vendor shall review the audit findings and take any additional corrective actions, to include re-auditing of the deficient areas where indicated, to preclude repetition of the condition.

(7) Licensees and applicants may jointly conduct audits, or may accept audits of the contractors or vendors that were conducted by other licensees and applicants who are subject to this section, if the audit addresses the services obtained from the contractor or vendor by each of the sharing licensees and applicants. The contractors or vendors may jointly conduct audits, or may accept audits of its subcontractors that were conducted by other licensees, applicants, or contractors or vendors who are subject to this section, if the audit addresses the services obtained from the subcontractor by each of the sharing licensees, applicants, and the contractors or vendors.

(i) Licensees, applicants, and contractors or vendors shall review audit records and reports to identify any areas that were not covered by the shared or accepted audit and ensure that authorization program elements and services upon which the licensee, applicant, or contractor or vendor relies are audited, if the program elements and services were not addressed in the shared audit.

(ii) Sharing licensees and applicants need not re-audit the same contractor or vendor for the same time. Sharing contractors or vendors need not re-audit the same subcontractor for the same time.

(iii) Sharing licensees, applicants, and contractors or vendors shall maintain a copy of the shared audits, including findings, recommendations, and corrective actions.

(o) *Records.* Licensee, applicants, and contractors or vendors shall maintain the records that are required by the regulations in this section for the period specified by the appropriate regulation. If a retention period is not otherwise specified, these records must be retained until the Commission terminates the facility's license, certificate, or other regulatory approval.

(1) Records may be stored and archived electronically, provided that the method used to create the electronic records meets the following criteria:

(i) Provides an accurate representation of the original records;

(ii) Prevents unauthorized access to the records;

(iii) Prevents the alteration of any archived information and/or data once it has been committed to storage; and

(iv) Permits easy retrieval and recreation of the original records.

(2) Licensees and applicants who are subject to this section shall retain the following records:

(i) Records of the information that must be collected under paragraphs (d) and (e) of this section that results in the granting of unescorted access or certifying of unescorted access authorization for at least 5 years after the licensee or applicant terminates or denies an individual's unescorted access or unescorted access authorization or until the completion of all related legal proceedings, whichever is later;

(ii) Records pertaining to denial or unfavorable termination of unescorted access or unescorted access authorization and related management actions for at least 5 years after the licensee or applicant terminates or denies an individual's unescorted access or unescorted access authorization or until the completion of all related

legal proceedings, whichever is later; and

(iii) Documentation of the granting and termination of unescorted access or unescorted access authorization for at least 5 years after the licensee or applicant terminates or denies an individual's unescorted access or unescorted access authorization or until the completion of all related legal proceedings, whichever is later. Contractors or vendors may maintain the records that are or were pertinent to granting, certifying, denying, or terminating unescorted access or unescorted access authorization that they collected for licensees or applicants. If the contractors or vendors maintain the records on behalf of a licensee or an applicant, they shall follow the record retention requirement specified in this section. Upon termination of a contract between the contractor and vendor and a licensee or applicant, the contractor or vendor shall provide the licensee or applicant with all records collected for the licensee or applicant under this chapter.

(3) Licensees, applicants, and contractors or vendors shall retain the following records for at least 3 years or until the completion of all related proceedings, whichever is later:

(i) Records of behavioral observation training conducted under paragraph (f)(2) of this section; and

(ii) Records of audits, audit findings, and corrective actions taken under paragraph (n) of this section.

(4) Licensees, applicants, and contractors or vendors shall retain written agreements for the provision of services under this section, for three years after termination or completion of the agreement, or until completion of all proceedings related to a denial or unfavorable termination of unescorted access or unescorted access authorization that involved those services, whichever is later.

(5) Licensees, applicants, and contractors or vendors shall retain records of the background investigations, psychological assessments, supervisory reviews, and behavior observation program actions related to access authorization program personnel, conducted under paragraphs (d) and (e) of this section, for the length of the individual's employment by or contractual relationship with the licensee, applicant, or the contractor or vendor and three years after the termination of employment, or until the completion of any proceedings relating to the actions of such access authorization program personnel, whichever is later.

(6) Licensees, applicants, and the contractors or vendors who have been authorized to add or manipulate data that is shared with licensees subject to this section shall ensure that data linked to the information about individuals who have applied for unescorted access or unescorted access authorization, which is specified in the licensee's or applicant's access authorization program documents, is retained.

(i) If the shared information used for determining individual's trustworthiness and reliability changes or new or additional information is developed about the individual, the licensees, applicants, and the contractors or vendors that acquire this information shall correct or augment the data and ensure it is shared with licensees subject to this section. If the changed, additional or developed information has implications for adversely affecting an individual's trustworthiness and reliability, the licensee, applicant, or the contractor or vendor who discovered or obtained the new, additional or changed information, shall, on the day of discovery, inform the reviewing official of any licensee or applicant access authorization program under which the individual is maintaining his or her unescorted access or unescorted access authorization status of the updated information.

(ii) The reviewing official shall evaluate the shared information and take appropriate actions, which may include denial or unfavorable termination of the individual's unescorted access authorization. If the notification of change or updated information cannot be made through usual methods, licensees, applicants, and the contractors or vendors shall take manual actions to ensure that the information is shared as soon as reasonably possible. Records maintained in any database(s) must be available for NRC review.

(7) If a licensee or applicant administratively withdraws an individual's unescorted access or unescorted access authorization status caused by a delay in completing any portion of the background investigation or for a licensee or applicant initiated evaluation, or reevaluation that is not under the individual's control, the licensee or applicant shall record this administrative action to withdraw the individual's unescorted access or unescorted access authorization with other licensees subject to this section. However, licensees and applicants shall not document this administrative withdrawal as denial or unfavorable termination and shall not respond to a suitable inquiry conducted under the provisions of 10 CFR parts 26, a background investigation conducted under the provisions of this section, or any other inquiry or investigation as denial nor unfavorable termination. Upon favorable completion of the background investigation element that caused the administrative withdrawal, the licensee or applicant shall immediately ensure that any matter that could link the individual to the administrative action is eliminated from the subject individual's access authorization or personnel record and other records, except if a review of the information obtained or developed causes the reviewing official to unfavorably terminate or deny the individual's unescorted access.

[74 FR 13979, Mar. 27, 2009, as amended at 77 FR 39909, July 6, 2012, 81 FR 86910, Dec. 2, 2016]

§ 73.57 Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to Safeguards Information.

(a) *General.* (1) Each licensee who is authorized to engage in an activity subject to regulation by the Commission shall comply with the requirements of this section.

(2) Each applicant for a license to engage in an activity subject to regulation by the Commission, as well as each entity who has provided written notice to the Commission of intent to file an application for licensing, certification, permitting, or approval of a product subject to regulation by the Commission shall submit fingerprints for those individuals who will have access to Safeguards Information.

(3) Before receiving its operating license under 10 CFR part 50 or before the Commission makes its finding under § 52.103(g) of this chapter, each applicant for a license to operate a nuclear power reactor (including an applicant for a combined license) or a non-power reactor may submit fingerprints for those individuals who will require unescorted access to the nuclear power facility or non-power reactor facility.

(b) *General performance objective and requirements.* (1) Except those listed in paragraph (b)(2) of this section, each licensee subject to the provisions of this section shall fingerprint each individual who is permitted unescorted access to the nuclear power facility, the non-power reactor facility in accordance with paragraph (g) of this section, or access to Safeguards Information. The licensee will then review and use the information received from the Federal Bureau of Investigation (FBI) and, based on the provisions contained in this section, determine either to continue to grant or to deny further unescorted access to the nuclear power facility, the non-power reactor facility, or access to Safeguards Information for that individual. Individuals who do not have unescorted access or access to Safeguards Information shall be fingerprinted by the licensee and the results of the criminal history records check shall be used before making a determination for granting unescorted access to the nuclear power facility, non-power reactor facility, or to Safeguards Information.

(2) Licensees need not fingerprint in accordance with the requirements of this section for the following categories:

(i) For unescorted access to the nuclear power facility or the non-power reactor facility (but must adhere to provisions contained in §§ 73.21 and 73.22): NRC employees and NRC contractors on official agency business; individuals responding to a site emergency in accordance with the provisions of § 73.55(a); offsite emergency response personnel who are responding to an emergency at a non-power reactor

facility; a representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement at designated facilities who has been certified by the NRC; law enforcement personnel acting in an official capacity; Federal, State or local government employees who have had equivalent reviews of FBI criminal history data; and individuals employed at a facility who possess ''Q'' or ''L'' clearances or possess another active government granted security clearance (*i.e.*, Top Secret, Secret, or Confidential);

(ii) For access to Safeguards Information only but must adhere to provisions contained in §§ 73.21, 73.22, and 73.23: the categories of individuals specified in 10 CFR 73.59.

(iii) Any licensee currently processing criminal history requests through the FBI pursuant to Executive Order 13467, as amended by Executive Order 13764, need not also submit such requests to the NRC under this section; and

(iv) Upon further notice to licensees and without further rulemaking, the Commission may waive certain requirements of this section on a temporary basis.

(v) Individuals who have a valid unescorted access authorization to a non-power reactor facility on November 7, 2012 are not required to undergo a new fingerprint-based criminal history records check pursuant to paragraph (g) of this section, until such time that the existing authorization expires, is terminated, or is otherwise to be renewed.

(3) The licensee shall notify each affected individual that the fingerprints will be used to secure a review of his/her criminal history record, and inform the individual of proper procedures for revising the record or including explanation in the record.

(4) Fingerprinting is not required if the licensee is reinstating the unescorted access to the nuclear power facility, the non-power reactor facility, or access to Safeguards Information granted an individual if:

(i) The individual returns to the same nuclear power utility or non-power reactor facility that granted access and such access has not been interrupted for a continuous period of more than 365 days; and

(ii) The previous access was terminated under favorable conditions.

(5) Fingerprints need not be taken, in the discretion of the licensee, if an individual who is an employee of a licensee, contractor, manufacturer, or supplier has been granted unescorted access to a nuclear power facility, a non-power reactor facility, or to Safeguards Information by another licensee, based in part on a criminal history records check under this section. The criminal history records check file may be transferred to the gaining licensee in accordance with the provisions of paragraph (f)(3) of this section.

(6) All fingerprints obtained by the licensee under this section must be submitted to the Attorney General of the United States through the Commission.

(7) The licensee shall review the information received from the Attorney General and consider it in making a determination for granting unescorted access to the individual or access to Safeguards Information.

(8) A licensee shall use the information obtained as part of a criminal history records check solely for the purpose of determining an individual's suitability for unescorted access to the nuclear power facility, the non-power reactor facility, or access to Safeguards Information.

(c) *Prohibitions.* (1) A licensee may not base a final determination to deny an individual unescorted access to the nuclear power facility, the non-power reactor facility, or access to Safeguards Information solely on the basis of information received from the FBI involving:

(i) An arrest more than 1 year old for which there is no information of the disposition of the case; or

(ii) An arrest that resulted in dismissal of the charge or an acquittal.

(2) A licensee may not use information received from a criminal history check obtained under this section in a manner that would infringe upon the rights of any individual under the First Amendment to the Constitution of the United States, nor shall the licensee use the information in any way which would discriminate among individuals

on the basis of race, religion, national origin, sex, or age.

(d) *Procedures for processing of fingerprint checks.* (1) For the purpose of complying with this section, licensees shall, using an appropriate method listed in § 73.4, submit to the NRC's Division of Physical and Cyber Security Policy, Mail Stop T–07D04M , one completed, legible standard fingerprint card (Form FD–258, ORIMDNRCOOOZ) or, where practicable, other fingerprint records for each individual requiring unescorted access to the nuclear power facility, the non-power reactor facility, or access to Safeguards Information, to the Director of the NRC's Division of Physical and Cyber Security Policy, marked for the attention of the Division's Criminal History Check Section. Copies of these forms may be obtained by writing the Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, by calling 301–415–5877, or by email to *FORMS.Resource@nrc.gov*. Guidance on what alternative formats might be practicable is referenced in § 73.4. The licensee shall establish procedures to ensure that the quality of the fingerprints taken results in minimizing the rejection rate of fingerprint cards due to illegible or incomplete cards.

(2) The Commission will review applications for criminal history checks for completeness. Any Form FD–258 or other fingerprint record containing omissions or evident errors will be returned to the licensee for corrections. The fee for processing fingerprint checks includes one free resubmission if the initial submission is returned by the FBI because the fingerprint impressions cannot be classified. The one free resubmission must have the FBI Transaction Control Number reflected on the resubmission. If additional submissions are necessary, they will be treated as an initial submittal and require a second payment of the processing fee. The payment of a new processing fee entitles the submitter to an additional free resubmittal, if necessary. Previously rejected submissions may not be included with the third submission because the submittal will be rejected automatically.

(3)(i) Fees for the processing of fingerprint checks are due upon application. Licensees shall submit payment with the application for the processing of fingerprints through corporate check, certified check, cashier's check, money order, or electronic payment, made payable to ''U.S. NRC.'' (For guidance on making electronic payments, contact the Security Branch, Division of Facilities and Security, at (301) 415–7404). Combined payment for multiple applications is acceptable.

(ii) The application fee is the sum of the user fee charged by the FBI for each fingerprint card or other fingerprint record submitted by the NRC on behalf of a licensee, and an administrative processing fee assessed by the NRC. The NRC processing fee covers administrative costs associated with NRC handling of licensee fingerprint submissions. The Commission publishes the amount of the fingerprint records check application fee on the NRC public Web site. (To find the current fee amount, go to the Electronic Submittals page at *http://www.nrc.gov/site-help/e-submittals.html* and see the link for the Criminal History Program.) The Commission will directly notify licensees who are subject to this regulation of any fee changes.

(4) The Commission will forward to the submitting licensee all data received from the FBI as a result of the licensee's application(s) for criminal history checks, to include the FBI fingerprint record.

(e) *Right to correct and complete information.* (1) Prior to any final adverse determination, the licensee shall make available to the individual the contents of records obtained from the FBI for the purpose of assuring correct and complete information. Confirmation of receipt by the individual of this notification must be maintained by the licensee for a period of 1 year from the date of the notification.

(2) If after reviewing the record, an individual believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating (of the alleged deficiency), or to explain any matter in the record, the individual may initiate challenge procedures. These procedures include direct

application by the individual challenging the record to the agency, *i.e.*, law enforcement agency, that contributed the questioned information or direct challenge as to the accuracy or completeness of any entry on the criminal history record to the Federal Bureau of Investigation Criminal Investigative Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26537-9700 as set forth in 28 CFR 16.30 through 16.34. In the latter case, the FBI then forwards the challenge to the agency that submitted the data requesting that agency to verify or correct the challenged entry. Upon receipt of an official communication directly from the agency that contributed the original information, the FBI Criminal Justice Information Services Division makes any changes necessary in accordance with the information supplied by that agency. Licensees must provide at least 10 days for an individual to initiate action to challenge the results of an FBI criminal history records check after the record being made available for his/her review. The licensee may make a final adverse determination based upon the criminal history record, if applicable, only upon receipt of the FBI's confirmation or correction of the record.

(3) In addition to the right to obtain records from the FBI in paragraph (e)(1) of this section and the right to initiate challenge procedures in paragraph (e)(2) of this section, an individual participating in an NRC adjudication and seeking to obtain Safeguards Information for use in that adjudication may appeal a final adverse determination by the NRC Office of Administration to the presiding officer of the proceeding. The request may also seek to have the Chief Administrative Judge designate an officer other than the presiding officer of the proceeding to review the adverse determination.

(f) *Protection of information.* (1) Each licensee who obtains a criminal history record on an individual under this section shall establish and maintain a system of files and procedures for protection of the record and the personal information from unauthorized disclosure.

(2) The licensee may not disclose the record or personal information collected and maintained to persons other than the subject individual, his/her representative, or to those who have a need to have access to the information in performing assigned duties in the process of granting or denying unescorted access to the nuclear power facility, the non-power reactor facility or access to Safeguards Information. No individual authorized to have access to the information may re-disseminate the information to any other individual who does not have a need to know.

(3) The personal information obtained on an individual from a criminal history record check may be transferred to another licensee:

(i) Upon the individual's written request to the licensee holding the data to re-disseminate the information contained in his/her file; and

(ii) The gaining licensee verifies information such as name, date of birth, social security number, sex, and other applicable physical characteristics for identification.

(4) The licensee shall make criminal history records obtained under this section available for examination by an authorized representative of the NRC to determine compliance with the regulations and laws.

(5) The licensee shall retain all fingerprint and criminal history records received from the FBI, or a copy if the individual's file has been transferred, on an individual (including data indicating no record) for one year after termination or denial of unescorted access to the nuclear power facility, the non-power reactor facility, or access to Safeguards Information.

(g) *Fingerprinting requirements for unescorted access for non-power reactor licensees.* (1) No person shall be permitted unescorted access to a non-power reactor facility unless that person has been determined by an NRC-approved reviewing official to be trustworthy and reliable based on the results of an FBI fingerprint-based criminal history records check obtained in accordance with this paragraph. The reviewing official is required to have unescorted access in accordance with this section or access to Safeguards Information.

(2) Each non-power reactor licensee subject to the requirements of this section shall obtain the fingerprints for a criminal history records check for each individual who is seeking or permitted:

(i) Unescorted access to vital areas of the non-power reactor facility; or

(ii) Unescorted access to special nuclear material in the non-power reactor facility provided the individual who is seeking or permitted unescorted access possesses the capability and knowledge to make unauthorized use of the special nuclear material in the non-power reactor facility or to remove the special nuclear material from the non-power reactor in an unauthorized manner.

[52 FR 6314, Mar. 2, 1987; 52 FR 7821, Mar. 13, 1987]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting §73.57, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at *www.govinfo.gov*.

§ 73.58 Safety/security interface requirements for nuclear power reactors.

(a) Each operating nuclear power reactor licensee with a license issued under part 50 or 52 of this chapter shall comply with the requirements of this section.

(b) The licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to plant configurations, facility conditions, or security.

(c) The scope of changes to be assessed and managed must include planned and emergent activities (such as, but not limited to, physical modifications, procedural changes, changes to operator actions or security assignments, maintenance activities, system reconfiguration, access modification or restrictions, and changes to the security plan and its implementation).

(d) Where potential conflicts are identified, the licensee shall communicate them to appropriate licensee personnel and take compensatory and/or mitigative actions to maintain safety and security under applicable Commission regulations, requirements, and license conditions.

[74 FR 13987, Mar. 27, 2009]

§ 73.59 Relief from fingerprinting, identification and criminal history records checks and other elements of background checks for designated categories of individuals.

Fingerprinting, and the identification and criminal history records checks required by section 149 of the Atomic Energy Act of 1954, as amended, and other elements of background checks are not required for the following individuals prior to granting access to Safeguards Information, including Safeguards Information designated as Safeguards Information-Modified Handling as defined in 10 CFR 73.2:

(a) An employee of the Commission or the Executive Branch of the United States government who has undergone fingerprinting for a prior U.S. government criminal history records check;

(b) A member of Congress;

(c) An employee of a member of Congress or Congressional committee who has undergone fingerprinting for a prior U.S. government criminal history records check;

(d) The Comptroller General or an employee of the Government Accountability Office who has undergone fingerprinting for a prior U.S. Government criminal history records check;

(e) The Governor of a State or his or her designated State employee representative;

(f) A representative of a foreign government organization that is involved in planning for, or responding to, nuclear or radiological emergencies or security incidents who the Commission approves for access to Safeguards Information, including Safeguards Information designated as Safeguards Information—Modified Handling;

(g) Federal, State, or local law enforcement personnel;

(h) State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives;

(i) Agreement State employees conducting security inspections on behalf of the NRC pursuant to an agreement executed under section 274.i. of the Atomic Energy Act of 1954, as amended;

(j) Representatives of the International Atomic Energy Agency (IAEA) engaged in activities associated

with the U.S./IAEA Safeguards Agreement who have been certified by the NRC;

(k) Any agent, contractor, or consultant of the aforementioned persons who has undergone equivalent criminal history records and background checks to those required by 10 CFR 73.22(b) or 73.23(b).

(l) Tribal official or the Tribal official's designated representative, and Tribal law enforcement personnel.

[73 FR 63580, Oct. 24, 2008, as amended at 77 FR 34206, June 11, 2012]

§ 73.60 Additional requirements for physical protection at nonpower reactors.

Each nonpower reactor licensee who, pursuant to the requirements of part 70 of this chapter, possesses at any site or contiguous sites subject to control by the licensee uranium–235 (contained in uranium enriched to 20 percent or more in the U–235 isotope), uranium–233, or plutonium, alone or in any combination in a quantity of 5000 grams or more computed by the formula, grams = (grams contained U–235) + 2.5 (grams U–233 + grams plutonium), shall protect the special nuclear material from theft or diversion pursuant to the requirements of paragraphs 73.67 (a), (b), (c), and (d), in addition to this section, except that a licensee is exempt from the requirements of paragraphs (a), (b), (c), (d), and (e) of this section to the extent that it possesses or uses special nuclear material that is not readily separable from other radioactive material and that has a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surface without intervening shielding.

(a) *Access requirements.* (1) Special nuclear material shall be stored or processed only in a material access area. No activities other than those which require access to special nuclear material or equipment employed in the process, use, or storage of special nuclear material, shall be permitted within a material access area.

(2) Material access areas shall be located only within a protected area to which access is controlled.

(3) Special nuclear material not in process shall be stored in a vault equipped with an intrusion alarm or in a vault-type room, and each such vault or vault-type room shall be controlled as a separate material access area.

(4) Enriched uranium scrap in the form of small pieces, cuttings, chips, solutions or in other forms which result from a manufacturing process, contained in 30-gallon or larger containers, with a uranium-235 content of less than 0.25 grams per liter, may be stored within a locked and separately fenced area which is within a larger protected area provided that the storage area is no closer than 25 feet to the perimeter of the protected area. The storage area when unoccupied shall be protected by a guard or watchman who shall patrol at intervals not exceeding 4 hours, or by intrusion alarms.

(5) Admittance to a material access area shall be under the control of authorized individuals and limited to individuals who require such access to perform their duties.

(6) Prior to entry into a material access area, packages shall be searched for devices such as firearms, explosives, incendiary devices, or counterfeit substitute items which could be used for theft or diversion of special nuclear material.

(7) Methods to observe individuals within material access areas to assure that special nuclear material is not diverted shall be provided and used on a continuing basis.

(b) *Exit requirement.* Each individual, package, and vehicle shall be searched for concealed special nuclear material before exiting from a material access area unless exit is into a contiguous material access area. The search may be carried out by a physical search or by use of equipment capable of detecting the presence of concealed special nuclear material.

(c) *Detection aid requirement.* Each unoccupied material access area shall be locked and protected by an intrusion alarm on active status. All emergency exits shall be continuously alarmed.

(d) *Testing and maintenance.* Each licensee shall test and maintain intrusion alarms, physical barriers, and other devices utilized pursuant to the requirements of this section as follows:

(1) Intrusion alarms, physical barriers, and other devices used for material protection shall be maintained in operable condition.

(2) Each intrusion alarm shall be inspected and tested for operability and required functional performance at the beginning and end of each interval during which it is used for material protection, but not less frequently than once every seven (7) days.

(e) *Response requirement.* Each licensee shall establish, maintain, and follow an NRC-approved safeguards contingency plan for responding to threats, thefts, and radiological sabotage related to the special nuclear material and 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.''

(f) In addition to the fixed-site requirements set forth in this section and in § 73.67, the Commission may require, depending on the individual facility and site conditions, any alternate or additional measures deemed necessary to protect against radiological sabotage at nonpower reactors licensed to operate at or above a power level of 2 megawatts thermal.

[38 FR 35430, Dec. 28, 1973, as amended at 44 FR 68199, Nov. 28, 1979; 57 FR 33431, July 29, 1992; 58 FR 13700, Mar. 15, 1993; 86 FR 43403, Aug. 9, 2021]

§ 73.61 Relief from fingerprinting and criminal history records check for designated categories of individuals permitted unescorted access to certain radioactive materials or other property.

Notwithstanding any other provision of the Commission's regulations, fingerprinting and the identification and criminal history records checks required by section 149 of the Atomic Energy Act of 1954, as amended, are not required for the following individuals prior to granting unescorted access to radioactive materials or other property that the Commission determines by regulation or order to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks:

(a) An employee of the Commission or of the Executive Branch of the U.S. Government who has undergone fingerprinting for a prior U.S. Government criminal history check;

(b) A Member of Congress;

(c) An employee of a member of Congress or Congressional committee who has undergone fingerprinting for a prior U.S. Government criminal history check;

(d) The Governor of a State or his or her designated State employee representative;

(e) Federal, State, or local law enforcement personnel;

(f) State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives;

(g) Agreement State employees conducting security inspections on behalf of the NRC pursuant to an agreement executed under section 274.i. of the Atomic Energy Act;

(h) Representatives of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who have been certified by the NRC.

[72 FR 4948, Feb. 2, 2007]

§ 73.67 Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance.

(a) *General performance objectives.* (1) Each licensee who possesses, uses or transports special nuclear material of moderate or low strategic significance shall establish and maintain a physical protection system that will achieve the following objectives:

(i) Minimize the possibilities for unauthorized removal of special nuclear material consistent with the potential consequences of such actions; and

(ii) Facilitate the location and recovery of missing special nuclear material.

(2) To achieve these objectives, the physical protection system shall provide:

(i) Early detection and assessment of unauthorized access or activities by an

external adversary within the controlled access area containing special nuclear material;

(ii) Early detection of removal of special nuclear material by an external adversary from a controlled access area;

(iii) Assure proper placement and transfer of custody of special nuclear material; and

(iv) Respond to indications of an unauthorized removal of special nuclear material and then notify the appropriate response forces of its removal in order to facilitate its recovery.

(b)(1) A licensee is exempt from the requirements of this section to the extent that he possesses, uses, or transports:

(i) Special nuclear material which is not readily separable from other radioactive material and which has a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surface without intervening shielding, or

(ii) Sealed plutonium-beryllium neutron sources totaling 500 grams or less contained plutonium at any one site or contiguous sites, or

(iii) Plutonium with an isotopic concentration exceeding 80 percent in plutonium-238.

(2) A licensee who has quantities of special nuclear material equivalent to special nuclear material of moderate strategic significance distributed over several buildings may, for each building which contains a quantity of special nuclear material less than or equal to a level of special nuclear material of low strategic significance, protect the material in that building under the lower classification physical security requirements.

(c) Each licensee who possesses, uses, transports, or delivers to a carrier for transport special nuclear material of moderate strategic significance, or 10 kg or more of special nuclear material of low strategic significance shall:

(1) Submit a security plan or an amended security plan describing how the licensee will comply with all the requirements of paragraphs (d), (e), (f), and (g) of this section, as appropriate, including schedules of implementation. The licensee shall retain a copy of the effective security plan as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the original plan was submitted. Copies of superseded material must be retained for three years after each change.

(2) Within 30 days after the plan submitted pursuant to paragraph (c)(1) of this section is approved, or when specified by the NRC in writing, implement the approved security plan.

(d) *Fixed site requirements for special nuclear material of moderate strategic significance.* Each licensee who possesses, stores, or uses quantities and types of special nuclear material of moderate strategic significance at a fixed site or contiguous sites, except as allowed by paragraph (b)(2) of this section and except those who are licensed to operate a nuclear power reactor pursuant to part 50, shall:

(1) Use the material only within a controlled access area which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities,

(2) Store the material only within a controlled access area such as a vault-type room or approved security cabinet or their equivalent which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities,

(3) Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetration or activities,

(4) Conduct screening prior to granting an individual unescorted access to the controlled access area where the material is used or stored, in order to obtain information on which to base a decision to permit such access,

(5) Develop and maintain a controlled badging and lock system to identify and limit access to the controlled access areas to authorized individuals,

(6) Limit access to the controlled access areas to authorized or escorted individuals who require such access in order to perform their duties,

(7) Assure that all visitors to the controlled access areas are under the constant escort of an individual who has been authorized access to the area,

(8) Establish a security organization or modify the current security organization to consist of at least one watchman per shift able to assess and respond to any unauthorized penetrations or activities in the controlled access areas,

(9) Provide a communication capability between the security organization and appropriate response force,

(10) Search on a random basis vehicles and packages leaving the controlled access areas, and

(11) Establish and maintain written response procedures for dealing with threats of thefts or thefts of these materials. The licensee shall retain a copy of the response procedures as a record for the period during which the licensee possesses the appropriate type and quantity of special nuclear material requiring this record under each license for which the original procedures were developed and, for three years thereafter. Copies of superseded material must be retained for three years after each change.

(e) *In-transit requirements for special nuclear material of moderate strategic significance.* (1) Each licensee who transports, exports or delivers to a carrier for transport special nuclear material of moderate strategic significance shall:

(i) Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification,

(ii) Receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport,

(iii) Check the integrity of the container and locks or seals prior to shipment, and

(iv) Arrange for the in-transit physical protection of the materials in accordance with the requirements of §73.67(e)(3) unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection.

(2) Each licensee who receives special nuclear material of moderate strategic significance shall:

(i) Check the integrity of the containers and seals upon receipt of the shipment,

(ii) Notify the shipper of receipt of the material as required in §74.15 of this chapter, and

(iii) Arrange for the in-transit physical protection of the material in accordance with the requirements of §73.67(e)(3) unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection.

(3) Each licensee who arranges for the in-transit physical protection of special nuclear material of moderate strategic significance, or who takes delivery of this material free on board (f.o.b.) the point at which it is delivered to a carrier for transport shall:

(i) Arrange for telephone or radio communications between the transport and the licensee or its designee: (A) To periodically confirm the status of the shipment (B) for notification of any delays in the scheduled shipment, and (C) to request appropriate local law enforcement agency response in the event of an emergency.

(ii) Minimize the time that the material is in transit by reducing the number and duration of nuclear material transfers and by routing the material in the most safe and direct manner,

(iii) Conduct screening of all licensee employees involved in the transportation of the material in order to obtain information on which to base a decision to permit them control over the material,

(iv) Establish and maintain written response procedures for dealing with threats of thefts or thefts of this material. The licensee shall retain a copy of the current response procedures as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the original procedures were developed and copies of superseded material must be retained for three years after each change.

(v) Make arrangements to be notified immediately of the arrival of the shipment at its destination, or of any such shipment that is lost or unaccounted

for after the estimated time of arrival at its destination, and

(vi) Initiate immediately a trace investigation of any shipment that is determined to be lost or unaccounted for after a reasonable time beyond the estimated arrival time.

(vii) Notify the NRC Operations Center after the discovery of the loss of the shipment and after recovery of or accounting for such lost shipment, in accordance with the provisions of §§ 73.1200 and 73.1205 of this part.

(4) Each licensee who arranges the physical protection of strategic special nuclear material in quantities of moderate strategic significance while in transit or who takes delivery of this material free on board (f.o.b.) the point at which it is delivered to a carrier for transport shall comply with the requirements of paragraphs (e) (1), (2), and (3) of this section. The licensee shall retain each record required by paragraphs (e) (1), (2), (3), and (4) (i) and (ii) of this section for three years after close of period licensee possesses special nuclear material under each license that authorizes these licensee activities. Copies of superseded material must be retained for three years after each change. In addition, the licensee shall—

(i) Make all shipments of the material either (A) in dedicated transports with no intermediate stops to load or unload other cargo and with no carrier or vehicle transfers or temporary storage in-transit, or (B) under arrangements whereby the custody of the shipment and all custody transfers are acknowledged by signature, and

(ii) Maintain the material under lock or under the control of an individual who has acknowledged acceptance of custody of the material by signature.

(5) Each licensee who exports special nuclear material of moderate strategic significance shall comply with the requirements specified in paragraphs (c) and (e) (1), (3), and (4) of this section. The licensee shall retain each record required by these sections for three years after the close of period for which the licensee possesses the special nuclear material under each license that authorizes the licensee to export this material. Copies of superseded material must be retained for three years after each change.

(6) Each licensee who imports special nuclear material of moderate strategic significance shall,

(i) Comply with the requirements specified in paragraphs (c) and (e) (2), (3), and (4) of this section. The licensee shall retain each record required by these sections for three years after the close of period for which the licensee possesses the special nuclear material under each license that authorizes the licensee to import this material. Copies of superseded material must be retained for three years after each change.

(ii) Notify the exporter who delivered the material to a carrier for transport of the arrival of such material.

(7) If, after receiving advance notice pursuant to § 73.72 from a licensee planning to import, export, transport, deliver to a carrier for transport in a single shipment, or take delivery at the point where it is delivered to a carrier, special nuclear material of moderate strategic significance containing in any part strategic special nuclear material, it appears to the Commission that two or more shipments of special nuclear material of moderate strategic significance, constituting in the aggregate an amount equal to or greater than a formula quantity of strategic special nuclear material, may be en route at the same time, the Commission may order one or more of the shippers to delay shipment according to the following provisions:

(i) The shipper shall provide to the Commission, upon request, such additional information regarding a planned shipment as the Commission considers pertinent to the decision on whether to delay such shipment.

(ii) The receiver of each shipment, or the shipper if the receiver is not a licensee, shall notify the Director, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response, by telephone, no later than 24 hours after arrival of such shipment at its final destination, or after such shipment has left the United States as an export, to confirm the integrity of the shipment at the time of receipt or exit from the United States.

(iii) The Commission shall notify the affected shippers no later than two days before the scheduled shipment date that a given shipment is to be delayed.

(iv) Shipments of special nuclear material of moderate strategic significance which are protected in accordance with the provisions of §§ 73.20, 73.25, and 73.26 shall not be subject to orders to delay shipment nor considered to constitute a portion of an aggregate formula quantity of strategic special nuclear material for the purposes of determining whether any shipments must delayed.

(f) *Fixed site requirements for special nuclear material of low strategic significance.* Each licensee who possesses, stores, or uses special nuclear material of low strategic significance at a fixed site or contiguous sites, except those who are licensed to operate a nuclear power reactor pursuant to part 50, shall:

(1) Store or use the material only within a controlled access area,

(2) Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetrations or activities,

(3) Assure that a watchman or offsite response force will respond to all unauthorized penetrations or activities, and

(4) Establish and maintain response procedures for dealing with threats of thefts or thefts of this material. The licensee shall retain a copy of the current response procedures as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the procedures were established. Copies of superseded material must be retained for three years after each change.

(g) *In-transit requirements for special nuclear material of low strategic significance.* (1) Each licensee who transports or who delivers to a carrier for transport special nuclear material of low strategic significance shall:

(i) Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification,

(ii) Receive confirmation from the receiver prior to commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport,

(iii) Transport the material in a tamper indicating sealed container,

(iv) Check the integrity of the containers and seals prior to shipment, and

(v) Arrange for the in-transit physical protection of the material in accordance with the requirements of § 73.67(g)(3) of this part, unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection.

(2) Each licensee who receives quantities and types of special nuclear material of low strategic significance shall:

(i) Check the integrity of the containers and seals upon receipt of the shipment,

(ii) Notify the shipper of receipt of the material as required in § 74.15 of this chapter, and

(iii) Arrange for the in-transit physical protection of the material in accordance with the requirements of § 73.67(g)(3) of this part, unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection.

(3) Each licensee, either shipper or receiver, who arranges for the physical protection of special nuclear material of low strategic significance while in transit or who takes delivery of such material free on board (f.o.b.) the point at which it is delivered to a carrier for transport shall:

(i) Establish and maintain response procedures for dealing with threats or thefts of this material. The licensee shall retain a copy of the current response procedures as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the procedures were established. Copies of superseded material must be retained for three years after each change.

(ii) Make arrangements to be notified immediately of the arrival of the shipment at its destination, or of any such

shipment that is lost or unaccounted for after the estimated time of arrival at its destination, and

(iii) Conduct immediately a trace investigation of any shipment that is lost or unaccounted for after the estimated arrival time and notify the NRC Headquarters Operations Center by telephone at the numbers specified in appendix A to this part within 1 hour after the discovery of the loss of the shipment and within 1 hour after recovery of or accounting for such lost shipment in accordance with the provisions of § 73.71 of this part.

(4) Each licensee who exports special nuclear material of low strategic significance shall comply with the appropriate requirements specified in paragraphs (c) and (g) (1) and (3) of this section. The licensee shall retain each record required by these sections for three years after the close of period for which the licensee possesses the special nuclear material under each license that authorizes the licensee to export this material. Copies of superseded material must be retained for three years after each change.

(5) Each licensee who imports special nuclear material of low strategic significance shall:

(i) Comply with the requirements specified in paragraphs (c) and (g) (2) and (3) of this section and retain each record required by these paragraphs for three years after the close of period for which the licensee possesses the special nuclear material under each license that authorizes the licensee to import this material. Copies of superseded material must be retained for three years after each change.

(ii) Notify the person who delivered the material to a carrier for transport of the arrival of such material.

[44 FR 43283, July 24, 1979. Redesignated at 44 FR 68198, Nov. 28, 1979, as amended at 45 FR 19215, Mar. 25, 1980; 47 FR 19114, May 4, 1982; 52 FR 21657, June 9, 1987; 53 FR 19260, May 27, 1988; 57 FR 33431, July 29, 1992, 59 FR 14087, Mar. 25, 1994; 67 FR 3586, Jan. 25, 2002; 67 FR 78143, Dec. 23, 2002; 68 FR 14530, Mar. 26, 2003; 68 FR 23575, May 5, 2003; 73 FR 32463, June 9, 2008; 74 FR 62684, Dec. 1, 2009; 83 FR 58723, Nov. 21, 2018; 85 FR 65664, Oct. 16, 2020; 86 FR 43403, Aug. 9, 2021; 88 FR 15891, Mar. 14, 2023]

Subpart H—Records and Postings

SOURCE: 88 FR 15801, Mar. 14, 2023, unless otherwise noted.

§ 73.70 Records.

Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records. Each licensee subject to the provisions of §§ 73.20, 73.25, 73.26, 73.27, 73.45, 73.46, 73.55, or 73.60 shall keep the following records:

(a) Names and addresses of all individuals who have been designated as authorized individuals. The licensee shall retain this record of currently designated authorized individuals for the period during which the licensee possesses the appropriate type and quantity of special nuclear material requiring this record under each license that authorizes the activity that is subject to the recordkeeping requirement and, for three years thereafter. Copies of superseded material must be retained for three years after each change.

(b) Names, addresses, and badge numbers of all individuals authorized to have access to vital equipment or special nuclear material, and the vital areas and material access areas to which authorization is granted. The licensee shall retain the record of individuals currently authorized this access for the period during which the licensee possesses the appropriate type and quantity of special nuclear material requiring this record under each license that authorizes the activity that

is subject to the recordkeeping requirement and, for three years thereafter. Copies of superseded material must be retained for three years after each change.

(c) A register of visitors, vendors, and other individuals not employed by the licensee pursuant to §§ 73.46(d)(13), 73.55(g)(7), or 73.60. The licensee shall retain this register as a record, available for inspection, for 3 years after the last entry is made in the register.

(d) A log indicating name, badge number, time of entry, and time of exit of all individuals granted access to a vital area except those individuals entering or exiting the reactor control room. The licensee shall retain this log as a record for three years after the last entry is made in the log.

(e) Documentation of all routine security tours and inspections, and of all tests, inspections, and maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security related equipment used pursuant to the requirements of this part. The licensee shall retain the documentation for these events for three years from the date of documenting each event.

(f) A record at each onsite alarm annunciation location of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, alarm circuit, date, and time. In addition, details of response by facility guards and watchmen to each alarm, intrusion, or other security incident shall be recorded. The license shall retain each record for three years after the record is made.

(g) Shipments of special nuclear material subject to the requirements of this part, including names of carriers, major roads to be used, flight numbers in the case of air shipments, dates and expected times of departure and arrival of shipments, verification of communication equipment on board the transfer vehicle, names of individuals who are to communicate with the transport vehicle, container seal descriptions and identification, and any other information to confirm the means utilized to comply with §§ 73.25, 73.26, and 73.27. This information must be recorded prior to shipment. Information obtained during the course of the shipment such as reports of all communications, change of shipping plan, including monitor changes, trace investigations, and others must also be recorded. The licensee shall retain each record about a shipment required by this paragraph (g) for three years after the record is made.

(h) Procedures for controlling access to protected areas and for controlling access to keys for locks used to protect special nuclear material. The licensee shall retain 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.

[53 FR 19261, May 27, 1988, as amended at 57 FR 33431, July 29, 1992; 83 FR 30288, June 28, 2018; 84 FR 63568, Nov. 18, 2019]

§ 73.71 [Reserved]

§ 73.72 Requirement for advance notice of shipment of formula quantities of strategic special nuclear material, special nuclear material of moderate strategic significance, or irradiated reactor fuel.

(a) A licensee, other than one specified in paragraph (b) of this section, who, in a single shipment, plans to deliver to a carrier for transport, to take delivery at the point where a shipment is delivered to a carrier for transport, to import, to export, or to transport a formula quantity of strategic special nuclear material, special nuclear material of moderate strategic significance, or irradiated reactor fuel[1] required to be protected in accordance with § 73.37, shall:

(1) Notify in writing by mail addressed to ATTN: Director, Office of Nuclear Security and Incident Response, U.S. Nuclear Regulatory Commission, Washington, DC 20555, or by using any appropriate method listed in § 73.4 of this part. Classified notifications shall be sent to the NRC headquarters classified mailing address listed in appendix A to this part.

[1] For purposes of 10 CFR 73.72, the terms ''irradiated reactor fuel'' as described in 10 CFR 73.37 and ''spent nuclear fuel'' are used interchangeably.

(2) Assure that the notification will be received at least 10 days before transport of the shipment commences at the shipping facility;

(3) Include the following information in the notification:

(i) The name(s), address(es), and telephone number(s) of the shipper, receiver, and carrier(s);

(ii) A physical description of the shipment:

(A) For a shipment other than irradiated fuel, the elements, isotopes, enrichment, and quantity;

(B) For a shipment of irradiated fuel, the physical form, quantity, type of reactor, and original enrichment;

(iii) A listing of the mode(s) of shipment, transfer point(s), and route(s) to be used;

(iv) The estimated time and date that shipment will commence and that each country along the route is scheduled to be entered; and

(v) The estimated time and date of arrival of the shipment at the destination;

(4) The NRC Headquarters Operations Center shall be notified about the shipment status by telephone at the phone numbers listed in appendix A to this part. Classified and safeguards notifications shall be made by secure telephone. The notifications shall take place at the following intervals:

(i) At least 2 days before commencement of the shipment;

(ii) Two hours before commencement of the shipment; and

(iii) Once the shipment is received at its destination.

(5) The NRC Headquarters Operations Center shall be notified by telephone of schedule changes of more than 6 hours at the phone numbers listed in appendix A to this part. Classified and safeguards notifications shall be made by secure telephone.

(b) A licensee who conducts an onsite transfer of spent nuclear fuel that does not travel upon or cross a public highway is exempt from the requirements of this section for that transfer.

[52 FR 9653, Mar. 26, 1987, as amended at 53 FR 4111, Feb. 12, 1988; 60 FR 24552, May 9, 1995; 67 FR 3586, Jan. 25, 2002; 68 FR 58820, Oct. 10, 2003; 74 FR 62684, Dec. 1, 2009; 78 FR 29557, May 20, 2013; 83 FR 58723, Nov. 21, 2018; 84 FR 63568, Nov. 18, 2019; 84 FR 67659, Dec. 11, 2019; 85 FR 65664, Oct. 16, 2020]

§ 73.73 Requirement for advance notice and protection of export shipments of special nuclear material of low strategic significance.

(a) A licensee authorized to export special nuclear material of low strategic significance shall:

(1) Notify in writing the Director, Office of Nuclear Security and Incident Response, by email (preferred method) to *AdvanceNotifications.Resource@nrc.gov* or by using any appropriate method listed in § 73.4;

(2) Assure that the notification will be received at least 10 days before transport of the shipment commences at the shipper's facility;

(3) Include the following information in the notification:

(i) The name(s), address(es), and telephone number(s) of the shipper, receiver, and carrier(s);

(ii) A physical description of the shipment (the elements, isotopes, form, etc.);

(iii) A listing of the mode(s) of shipment, transfer points, and routes to be used;

(iv) The estimated time and date that shipment will commence and that each country along the route is scheduled to be entered; and

(v) The estimated time and date of arrival of the shipment at the destination;

(4) Assure that during transport outside the United States, the shipment will be protected in accordance with Annex I to the Convention on the Physical Protection of Nuclear Material (see appendix E of this part).

(b) A licensee who needs to amend a written advance notification required by paragraph (a) of this section may notify the NRC Headquarters Operations Center by telephone at the numbers listed in appendix A to this part.

[52 FR 9653, Mar. 26, 1987, as amended at 53 FR 4112, Feb. 12, 1988; 60 FR 24553, May 9, 1995; 67 FR 3586, Jan. 25, 2002; 68 FR 58820, Oct. 10, 2003; 74 FR 62684, Dec. 1, 2009; 83 FR 58723, Nov. 21, 2018; 86 FR 67843, Nov. 30, 2021]

§ 73.74 Requirement for advance notice and protection of import shipments of nuclear material from countries that are not party to the Convention on the Physical Protection of Nuclear Material.

(a) A licensee authorized to import special nuclear material of low strategic significance from a country not a party to the Convention on the Physical Protection of Nuclear Material (*i.e.*, not listed in appendix F of this part) shall:

(1) Notify in writing the Director, Office of Nuclear Security and Incident Response, by email (preferred method) to *AdvanceNotifications.Resource@nrc.gov* or by using any appropriate method listed in § 73.4;

(2) Assure that the notification will be received at least 10 days before transport of the shipment commences at the shipper's facility; and

(3) Include the following information in the notification:

(i) The name(s), address(es) and telephone number(s) of the shipper, receiver, and carrier(s);

(ii) A physical description of the shipment (the isotopes, enrichment, quantity, etc.);

(iii) A listing of mode(s) of shipment, transfer points, and routes to be used;

(iv) The estimated time and date that shipment will commence and that each country along the route is scheduled to be entered; and

(v) The estimated time and date of arrival of the shipment at the destination.

(b) A licensee who needs to amend a written advance notification required by paragraph (a) of this section may notify the NRC Headquarters Operations Center by telephone at the numbers listed in appendix A to this part.

(c) A licensee authorized to import from a country not a party to the Convention on the Physical Protection of Nuclear Material (*i.e.*, not listed in appendix F of this part) a formula quantity of special nuclear material, special nuclear material of moderate strategic significance, special nuclear material of low strategic significance, or irradiated reactor fuel shall assure that during transport outside the United States the shipment will be protected in accordance with Annex I to the Convention on the Physical Protection of Nuclear Material (see appendix E of this part).

[52 FR 9654, Mar. 26, 1987, as amended at 53 FR 4112, Feb. 12, 1988; 60 FR 24553, May 9, 1995; 67 FR 3586, Jan. 25, 2002; 68 FR 58820, Oct. 10, 2003; 74 FR 62684, Dec. 1, 2009; 83 FR 58723, Nov. 21, 2018; 86 FR 67843, Nov. 30, 2021]

§ 73.75 Posting.

(a) This section applies to:

(1) Production or utilization facilities;

(2) High-level waste storage or disposal facilities and independent spent fuel storage installations;

(3) Uranium enrichment, uranium conversion, or nuclear fuel fabrication facilities.

(b)(1) Licensees or certificate holders operating facilities described in paragraph (a) of this section that have a protected area shall conspicuously post notices at every vehicle and pedestrian entrance to the protected area.

(2) Licensees or certificate holders operating facilities described in paragraph (a) of this section that include buildings not within a protected area that nonetheless contain special nuclear material, byproduct material, or source material shall conspicuously post notices at the personnel and vehicle entrances to each such building, except with respect to buildings for which no security plan is required under this part.

(3) The required notices must state: ''The willful unauthorized introduction of any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property into or upon these premises is a Federal crime. (42 U.S.C. 2278a.)''

(4) Every notice posted under this section must be easily readable day and night by both pedestrian and vehicular traffic entering the facility or installation.

(5) These notices may be combined with other notices.

(c) This section does not apply to facilities that, in addition to being regulated by the NRC under a license or certificate of compliance issued by the Commission, are also covered by U.S.

Department of Energy regulations imposing criminal penalties, and associated posting requirements, under section 229 of the Atomic Energy Act with respect to unauthorized introduction of dangerous weapons, explosives, or other dangerous instruments or materials likely to produce substantial injury or damage to persons or property.

[74 FR 52674, Oct. 14, 2009]

Subpart I—Enforcement

SOURCE: 88 FR 15891, Mar. 14, 2023, unless otherwise noted.

§ 73.77 Cyber security event notifications.

(a) Each licensee subject to the provisions of § 73.54 shall notify the NRC Headquarters Operations Center via the Emergency Notification System (ENS), in accordance with paragraph (c) of this section:

(1) Within one hour after discovery of a cyber attack that adversely impacted safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions within the scope of § 73.54.

(2) Within four hours:

(i) After discovery of a cyber attack that could have caused an adverse impact to safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications); or that could have compromised support systems and equipment, which if compromised, could have adversely impacted safety, security, or emergency preparedness functions within the scope of § 73.54.

(ii) After discovery of a suspected or actual cyber attack initiated by personnel with physical or electronic access to digital computer and communication systems and networks within the scope of § 73.54.

(iii) After notification of a local, State, or other Federal agency (e.g., law enforcement, FBI, etc.) of an event related to the licensee's implementation of their cyber security program for digital computer and communication systems and networks within the scope of § 73.54 that does not otherwise require a notification under paragraph (a) of this section.

(3) Within eight hours after receipt or collection of information regarding observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer and communication systems and networks within the scope of § 73.54.

(b) *Twenty-four hour recordable events.* (1) The licensee shall use the site corrective action program to record vulnerabilities, weaknesses, failures and deficiencies in their § 73.54 cyber security program within twenty-four hours of their discovery.

(2) The licensee shall use the site corrective action program to record notifications made under paragraph (a) of this section within twenty-four hours of their discovery.

(c) *Notification process.* (1) Each licensee shall make telephonic notifications required by paragraph (a) of this section to the NRC Headquarters Operations Center via the ENS. If the ENS is inoperative or unavailable, the licensee shall make the notification via a commercial telephone service or other dedicated telephonic system or any other methods that will ensure a report is received by the NRC Headquarters Operations Center within the timeframe. Commercial telephone numbers for the NRC Headquarters Operations Center are specified in appendix A to this part.

(2) Notifications required by this section that contain Safeguards Information may be made to the NRC Headquarters Operations Center without using secure communications systems under the exception in § 73.22(f)(3) for emergency or extraordinary conditions.

(3) Notifications required by this section that contain Safeguards Information and/or classified national security information and/or restricted data must be made to the NRC Headquarters Operations Center using secure communications systems appropriate to the sensitivity/classification level of

the message. Licensees making these types of telephonic notifications must contact the NRC Headquarters Operations Center at the commercial numbers specified in appendix A to this part and request a transfer to a secure telephone.

(i) If the licensee's secure communications capability is unavailable (e.g., due to the nature of the security event), the licensee must provide as much information to the NRC as is required by this section, without revealing or discussing any Safeguards Information and/or Classified Information, in order to meet the timeliness requirements of this section. The licensee must also indicate to the NRC that its secure communications capability is unavailable.

(ii) Licensees using a non-secure communications capability may be directed by the NRC Emergency Response management to provide classified information to the NRC over the non-secure system, due to the significance of the ongoing security event. In such circumstances, the licensee must document this direction and any information provided to the NRC over a non-secure communications capability in the written security follow-up report required in accordance with paragraph (d) of this section.

(4) For events reported under paragraph (a)(1) of this section, the NRC may request that the licensee maintain an open and continuous communication channel with the NRC Headquarters Operations Center.

(5) Licensees desiring to retract a previous security event report that has been determined to not meet the threshold of a reportable event must telephonically notify the NRC Headquarters Operations Center and indicate the report being retracted and basis for the retraction.

(6) *Declaration of emergencies.* Notifications made to the NRC for the declaration of an emergency class shall be performed in accordance with § 50.72 of this chapter, as applicable.

(7) *Elimination of duplication.* Separate notifications and reports are not required for events that are also reportable in accordance with §§ 50.72 and 50.73 of this chapter. However, these notifications should also indicate the applicable § 73.77 reporting criteria.

(d) *Written security follow-up reports.* Each licensee making an initial telephonic notification of security events to the NRC according to the provisions of paragraphs (a)(1), (a)(2)(i), and (a)(2)(ii) of this section must also submit a written security follow-up report to the NRC within 60 days of the telephonic notification in accordance with § 73.4.

(1) Licensees are not required to submit a written security follow-up report following a telephonic notification made under § 73.77(a)(2)(iii) or (a)(3).

(2) Each licensee shall submit to the NRC written security follow-up reports that are of a quality that will permit legible reproduction and processing.

(3) Licensees shall prepare the written security follow-up report on NRC Form 366.

(4) In addition to the addressees specified in § 73.4, the licensee shall also provide one copy of the written security follow-up report addressed to the Director, Office of Nuclear Security and Incident Response, or the Director's designee. Any written security follow-up reports containing classified information shall be transmitted to the NRC Headquarters' classified mailing address as specified in appendix A to this part.

(5) The written security follow-up report must include sufficient information for NRC analysis and evaluation.

(6) Significant supplemental information which becomes available after the initial telephonic notification to the NRC Headquarters Operations Center or after the submission of the written security follow-up report must be telephonically reported to the NRC Headquarters Operations Center under paragraph (c) of this section and also submitted in a revised written security follow-up report (with the revisions indicated) as required under this section.

(7) Errors discovered in a written security follow-up report must be corrected in a revised written security follow-up report with the revision(s) indicated.

(8) The revised written security follow-up report must replace the previous written security follow-up report; the update must be complete and not

be limited to only supplementary or revised information.

(9) If the licensee subsequently retracts a telephonic notification made under this section as not meeting the threshold of a reportable event, and has not yet submitted a written security follow-up report then submission of a written security follow-up report is not required.

(10) If the licensee subsequently retracts a telephonic notification made under this section as not meeting the threshold of a reportable event after it has submitted a written security follow-up report required by this paragraph, then the licensee shall submit a revised written security follow-up report in accordance with this paragraph.

(11) Each written security follow-up report submitted containing Safeguards Information or Classified Information must be created, stored, marked, labeled, handled, and transmitted to the NRC according to the requirements of §§ 73.21 and 73.22 or with part 95 of this chapter, as applicable.

(12) Each licensee shall maintain a copy of the written security follow-up report of an event submitted under this section as a record for a period of three years from the date of the report or until the Commission terminates the license for which the records were developed, whichever comes first.

[80 FR 67275, Nov. 2, 2015]

§ 73.80 Violations.

(a) The Commission may obtain an injunction or other court order to prevent a violation of the provisions of—

(1) The Atomic Energy Act of 1954, as amended;

(2) Title II of the Energy Reorganization Act of 1974, as amended; or

(3) A regulation or order issued pursuant to those Acts.

(b) The Commission may obtain a court order for the payment of a civil penalty imposed under section 234 of the Atomic Energy Act:

(1) For violations of—

(i) Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended:

(ii) Section 206 of the Energy Reorganization Act;

(iii) Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;

(iv) Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

(2) For any violation for which a license may be revoked under Section 186 of the Atomic Energy Act of 1954, as amended.

[57 FR 55078, Nov. 24, 1992]

§ 73.81 Criminal penalties.

(a) Section 223 of the Atomic Energy Act of 1954, as amended, provides for criminal sanctions for willful violation of, attempted violation of, or conspiracy to violate, any regulation issued under sections 161b, 161i, or 161o of the Act. For purposes of section 223, all the regulations in part 73 are issued under one or more of sections 161b, 161i, or 161o, except for the sections listed in paragraph (b) of this section.

(b) The regulations in part 73 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§ 73.1, 73.2, 73.3, 73.4, 73.5, 73.6, 73.8, 73.25, 73.45, 73.75, 73.80, and 73.81.

(c)(1) No person without authorization may carry, transport, or otherwise introduce or cause to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property into or upon a protected facility or installation. Willful violations of this provision are punishable by the criminal penalties set forth in sections 229b and 229c of the Atomic Energy Act of 1954, as amended.

(2) As used in this section:

(i) ''Protected facility or installation'' means any production or utilization facility, high-level waste storage or disposal facility, independent spent fuel storage installation, uranium enrichment, uranium conversion, or nuclear fuel fabrication facility, but does not include those portions of such facilities that are not required under § 73.75(b) of this part to be identified by notices posted at their pedestrian and vehicle entrances, and does not include facilities described in § 73.75(c) of this part.

(ii) ''Without authorization'' means not authorized as part of one's official duties to carry the weapon, explosive, or other instrument or material;

(iii) ''Dangerous weapon'' includes any firearm, as defined in either 18 U.S.C. 921 or 26 U.S.C. 5845, or dangerous weapon, as defined in 18 U.S.C. 930;

(iv) ''Explosive'' means any explosive as defined in 18 U.S.C. 844(j).

(3) An item, such as a dangerous weapon, explosive, or other dangerous instrument or material, is considered to have been carried, transported, or otherwise introduced or caused to be introduced into or upon a protected facility or installation for purposes of paragraph (c)(1) of this section once the item has traveled past a notice posted pursuant to §73.75 of this part at a vehicle or pedestrian entrance to the protected facility, or once the item has entered the protected facility or installation at a location that is not a vehicle or pedestrian entrance to the facility, whether such entry is accomplished through, over, under, or around a fence, wall, floor, roof, or other structural barrier enclosing the protected facility or installation or by any other means.

(4) For all protected facilities or installations that do not possess special nuclear material, byproduct material, or source material as of the effective date of this rule, this provision shall take effect upon receipt of such material at the applicable facility or installation.

[57 FR 55079, Nov. 24, 1992, as amended at 74 FR 52674, Oct. 14, 2009]

Subparts J–S [Reserved]

Subpart T—Security Notifications, Reports, and Recordkeeping

SOURCE: 88 FR 15891, Mar. 14, 2023, unless otherwise noted.

§73.1200 Notification of physical security events.

(a) *15-minute notifications—facilities.* Each licensee subject to the provisions of §73.20, §73.45, §73.46, §73.51, or §73.55 of this part must notify the NRC Headquarters Operations Center, as soon as possible but within 15 minutes after—

(1) The licensee's initiation of a security response in accordance with its safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against a licensee's facility; or

(2) The licensee's notification by law enforcement or government officials of a potential hostile action or act of sabotage anticipated within the next 12 hours against a licensee's facility.

(3) Licensee notifications to the NRC must:

(i) Identify the facility's name; and

(ii) Briefly describe the nature of the hostile action or event, including:

(A) The type of hostile action or event (e.g., armed assault, vehicle bomb, bomb threat, sabotage, etc.); and

(B) The current status (*i.e.,* imminent, in progress, or neutralized).

(4) Notifications must be made according to paragraph (o) of this section, as applicable.

(5) The licensee is not required to notify the NRC of security responses initiated as a result of threat or warning information communicated to the licensee from the NRC.

(6) The licensee's request for immediate local law enforcement agency (LLEA) assistance or initiation of a contingency response may take precedence over the notification to the NRC. However, in such instances, the licensee must notify the NRC as soon as possible thereafter.

(b) *15-minute notifications—shipments.* Each licensee subject to the provisions of §73.20, §73.25, §73.26, or §73.37 or its designated movement control center must notify the NRC Headquarters Operations Center, as soon as possible but within 15 minutes after—

(1) The licensee's initiation of a security response in accordance with its safeguards contingency plan or protective strategy, based on an imminent or actual hostile action against a shipment of Category I SSNM, spent nuclear fuel (SNF), or high-level radioactive waste (HLW); or

(2) The licensee's notification by law enforcement or government officials of a potential hostile action or attempted act of sabotage anticipated within less

than the next 12 hours against a shipment of Category I SSNM, SNF, or HLW.

(3) Licensee notifications to the NRC must:

(i) Identify the name of the facility making the shipment, the material being shipped, and the last known location of the shipment; and

(ii) Briefly describe the nature of the threat or event, including:

(A) Type of hostile threat or event (*e.g.*, armed assault, vehicle bomb, theft of shipment, sabotage, etc.); and

(B) Threat or event status (*i.e.*, imminent, in progress, or neutralized).

(4) Notifications must be made according to paragraph (o) of this section, as applicable.

(5) The licensee is not required to notify the NRC of security responses initiated as a result of threat or warning information communicated to the licensee from the NRC.

(6) The licensee's request for immediate LLEA assistance may take precedence over the notification to the NRC. However, in such instances, the licensee must notify the NRC as soon as possible thereafter.

(c) *One-hour notifications—facilities.* (1) Each licensee subject to the provisions of §73.20, §73.45, §73.46, §73.50, §73.51, §73.55, §73.60, or §73.67 must notify the NRC Headquarters Operations Center as soon as possible but no later than 1 hour after the time of discovery of the following significant facility security events involving—

(i) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause:

(A) The theft or diversion of a Category I, II, or III quantity of SSNM or a Category II or III quantity of special nuclear material (SNM);

(B) Significant physical damage to any nuclear power reactor, to a facility possessing a Category I or II quantity of SSNM, or to a facility storing or disposing of SNF and/or HLW;

(C) The unauthorized operation, manipulation, or tampering with any nuclear power reactor's controls or with structures, systems, and components (SSCs) that results in the interruption of normal operation of the reactor; or

(D) The unauthorized operation, manipulation, or tampering with any Category I SSNM facility's SSCs that results in an accidental criticality.

(ii)(A) For licensees required to have a vehicle barrier system protecting their facility, the introduction beyond the vehicle barrier of a quantity of unauthorized explosives that meets or exceeds the relevant facility's adversary characteristics.

(B) This provision is applicable to facilities where the vehicle barrier system protecting the facility is located at the Protected Area boundary.

(iii) The licensee's notification by law enforcement or government officials of a potential hostile action or act of sabotage anticipated within greater than 12 hours against a licensee's facility.

(2) Notifications must be made according to paragraph (o) of this section, as applicable.

(3) Notifications made under paragraph (a) of this section are not required to be repeated under this paragraph.

(4) As an exemption, licensees subject to §73.50, §73.60, or §73.67 are not required to make notifications for events listed under paragraph (c)(1)(iii) of this section.

(d) *One-hour notifications—shipments.* (1) Each licensee subject to the provisions of §73.20, §73.25, §73.26, §73.27, §73.37, or §73.67 or its designated movement control center must notify the NRC Headquarters Operations Center as soon as possible but no later than 1 hour after the time of discovery of the following significant transportation security events involving—

(i) Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a threat to commit or cause:

(A) The theft or diversion of the Category I, II, or III quantity of SSNM; a Category II or III quantity of SNM; SNF; or HLW being transported;

(B) Significant physical damage to any vehicle transporting a Category I or II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW; or

(C) Significant physical damage to the Category I or II quantity of SSNM,

a Category II quantity of SNM, SNF, or HLW being transported.

(ii) The discovery of the loss of a shipment of Category I SSNM.

(iii) The recovery of, or accounting for, a lost shipment of Category I SSNM.

(iv) The licensee's notification by law enforcement or government officials of a potential hostile action or attempted act of sabotage anticipated within greater than the next 12 hours against a shipment of Category I quantities of SSNM, SNF, or HLW.

(2) Notifications must be made according to paragraph (o) of this section, as applicable.

(3) Notifications made under paragraph (b) of this section are not required to be repeated under this paragraph.

(e) *Four-hour notifications—facilities.* (1) Each licensee subject to the provisions of §73.20, §73.45, §73.46, §73.50, §73.51, §73.55, §73.60, or §73.67 of this part must notify the NRC Headquarters Operations Center within 4 hours after time of discovery of the following facility security events involving—

(i) The actual access of an unauthorized person into a facility's protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA);

(ii) The attempted access of an unauthorized person into a PA, VA, MAA, or CAA;

(iii) The actual introduction of contraband into a PA, VA, or MAA;

(iv) The attempted introduction of contraband into a PA, VA, or MAA.

(v)(A) The discovery that a weapon that is authorized by the licensee's security plan is lost or uncontrolled within a PA, VA, or MAA;

(B) Uncontrolled authorized weapons are defined as weapons that are authorized by the licensee's security plan and are not in the possession of authorized personnel or are not in an authorized weapons storage location;

(vi) The unauthorized operation, manipulation, or tampering with any nuclear reactor or Category I SSNM facility's controls or SSCs that could prevent the implementation of the licensee's protective strategy for protecting any target set;

(vii) The identification or discovery of a previously unrecognized or unidentified vulnerability that could prevent the implementation of the licensee's protective strategy for protecting any target set; or

(viii)(A) For licensees required to have a vehicle barrier system protecting their facility, the identification or discovery at or beyond the vehicle barrier of unauthorized explosives.

(B) This provision is applicable to facilities where the vehicle barrier system protecting the facility is located at a distance from the Protected Area boundary greater than that assumed in the facility's blast analysis.

(2) An event related to the licensee's implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials provided that the event does not otherwise require a notification under paragraphs (a) through (h) of this section.

(3)(i) An event involving a law enforcement response to the facility that could reasonably be expected to result in public or media inquiries and that does not otherwise require a notification under paragraphs (a) through (h) of this section, or in other NRC regulations such as §50.72(b)(2)(xi) of this chapter.

(ii) As an exemption, licensees need not report law enforcement responses to minor incidents, such as traffic accidents.

(4) For licensees subject to the provisions of §73.55 of this part, an event involving the licensee's suspension of security measures.

(5) Notifications must be made according to paragraph (o) of this section, as applicable.

(6) Notifications made under paragraphs (a) and (c) of this section are not required to be repeated under this paragraph.

(f) *Four-hour notifications—shipments.* (1) Each licensee subject to the provisions of §73.20, §73.25, §73.26, §73.27, §73.37, or §73.67 or its designated movement control center must notify the NRC Headquarters Operations Center within 4 hours after time of discovery of the following transportation security events involving—

(i) The actual access of an unauthorized person into a transport vehicle transporting a Category I or II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW;

(ii) The attempted access of an unauthorized person into a transport vehicle transporting a Category I or II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW;

(iii) The actual access of an unauthorized person into the Category I or II quantity of SSNM, Category II quantity of SNM, SNF, or HLW being transported;

(iv) The attempted access of an unauthorized person into the Category I or II quantity of SSNM, Category II quantity of SNM, SNF, or HLW being transported;

(v) The actual introduction of contraband into a transport vehicle transporting a Category I or II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW;

(vi) The attempted introduction of contraband into a transport vehicle transporting a Category I or II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW;

(vii) The actual introduction of contraband into the Category I or II quantity of SSNM, Category II quantity of SNM, SNF, or HLW being transported;

(viii) The attempted introduction of contraband into the Category I or II quantity of SSNM, Category II quantity of SNM, SNF, or HLW being transported;

(ix) The discovery of the loss of a shipment of Category II or III quantities of SSNM, Category II or III quantities of SNM, SNF, or HLW; or

(x) The recovery of or accounting for a lost shipment of Category II or III quantities of SSNM, Category II or III quantities of SNM, SNF, or HLW.

(2) An event related to the licensee's implementation of their security program for which a notification was made to local, State, or Federal law enforcement officials, provided that the event does not otherwise require a notification under paragraphs (a) through (h) of this section.

(3) Notifications must be made according to paragraph (o) of this section, as applicable.

(4) Notifications made under paragraphs (b) and (d) of this section are not required to be repeated under this paragraph.

(g) *Eight-hour notifications—facilities.* (1) Each licensee subject to the provisions of §73.20, §73.45, §73.46, §73.50, §73.51, §73.55, §73.60, or §73.67 must notify the NRC Headquarters Operations Center within 8 hours after time of discovery of the following facility security program failures involving—

(i) Any failure, degradation, or vulnerability in a security or safeguards system, for which compensatory measures have not been employed within the required timeframe, that could allow unauthorized or undetected access of—

(A) Unauthorized personnel into a PA, VA, MAA, or CAA; or

(B) Contraband into a PA, VA, or MAA;

(ii) The unauthorized operation, manipulation, or tampering with any nuclear power reactor's controls or with SSCs that does not result in the interruption of normal operation of the reactor; or

(iii) The unauthorized operation, manipulation, or tampering with any Category I SSNM facility's SSCs that does not result in the interruption of normal operation of the facility or an accidental criticality.

(2) Notifications must be made according to paragraph (o) of this section, as applicable.

(3) Notifications made under paragraphs (a), (c), and (e) of this section are not required to be repeated under this paragraph.

(h) *Eight-hour notifications—shipments.* (1) Each licensee subject to the provisions of §73.20, §73.25, §73.26, §73.27, §73.37, or §73.67 or its designated movement control center must notify the NRC Headquarters Operations Center within 8 hours after time of discovery of the following transportation security program failures involving any failure, degradation, or vulnerability in a security or safeguards system, for which compensatory measures have not been employed within the required timeframe, that could allow unauthorized or undetected access of—

(i) Personnel or contraband into a transport vehicle transporting a Category I or II quantity of SSNM, a Category II quantity of SNM, SNF, or HLW; or

(ii) Personnel or contraband into the Category I or II quantity of SSNM, Category II quantity of SNM, SNF, or HLW being transported;

(2) Notifications must be made according to paragraph (o) of this section, as applicable.

(3) Notifications made under paragraphs (b), (d), and (f) of this section are not required to be repeated under this paragraph.

(i) through (l) [Reserved]

(m) *Enhanced weapons notifications—stolen or lost.* (1) Each licensee possessing enhanced weapons in accordance with §73.15 must—

(i) Immediately notify the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) upon discovery of any stolen or lost enhanced weapons (see 27 CFR 479.141).

(ii) Notify the NRC Headquarters Operations Center as soon as possible, but not later than 1 hour, after notification to the ATF of the discovery of any stolen or lost enhanced weapons possessed by the licensee.

(iii) Notify the appropriate local law enforcement agency (LLEA) officials as soon as possible, but not later than 48 hours, after the discovery of stolen or lost enhanced weapons. This notification must be made by telephone or in person to the appropriate LLEA officials. Licensees must include appropriate point of contact information in their security event notification procedures.

(2) Notifications to the NRC must be made according to paragraph (o) of this section, as applicable.

(n) *Enhanced weapons—adverse ATF findings.* (1) Each licensee possessing enhanced weapons in accordance with §73.15 must—

(i) Notify the NRC Headquarters Operations Center as soon as possible, but not later than 24 hours, after receipt of an adverse inspection finding, enforcement finding, or other adverse notice from the ATF regarding the licensee's possession, receipt, transfer, transportation, or storage of enhanced weapons; and

(ii) Notify the NRC Headquarters Operations Center as soon as possible, but not later than 24 hours after receipt of an adverse inspection finding, enforcement finding or other adverse notice from the ATF regarding any ATF issued Federal firearms license to the NRC licensee.

(2) Notifications must be made according to paragraph (o) of this section, as applicable.

(o) *Notification process.* (1) Each licensee must make the telephonic notifications to the NRC required by paragraphs (a) through (n) of this section to the NRC Headquarters Operations Center via any available telephone system. Commercial telephone numbers for the NRC Headquarters Operations Center are specified in Table 1 of appendix A of this part.

(2) Licensees must make required telephonic notifications via any method that will ensure that a report is received by the NRC Headquarters Operations Center or other specified government officials within the timeliness requirements of paragraphs (a) through (n) of this section, as applicable.

(3) Notifications required by this section that contain Safeguards Information may be made to the NRC Headquarters Operations Center without using secure communications systems under the exception of §73.22(f)(3) for the communication of emergency or extraordinary conditions.

(4)(i) Notifications required by this section that contain classified national security information and/or classified restricted data must be made to the NRC Headquarters Operations Center using secure communications systems appropriate to the classification level of the message. Licensees making classified telephonic notifications must contact the NRC Headquarters Operations Center at the commercial numbers specified in Table 1 of appendix A to this part and request a transfer to a secure telephone, as specified in paragraph III of appendix A to this part.

(ii) If the licensee's secure communications capability is unavailable (*e.g.*, due to the nature of the security event), the licensee must provide to the NRC the information required by this section, without revealing or discussing any classified information, in

order to meet the timeliness requirements of this section. The licensee must also indicate to the NRC that its secure communications capability is unavailable.

(iii) Licensees using a non-secure communications capability may be directed by the NRC emergency response management, in accordance with 32 CFR 2001.52(a), to provide classified national security information to the NRC over the non-secure system, due to the significance of the ongoing security event. In such circumstances, the licensee must document this direction and any information provided to the NRC over a non-secure communications capability in the follow-up written report required in accordance with § 73.1205.

(5) For events reported under paragraph (a) of this section, the NRC may request that the licensee establish and maintain an open and continuous communications channel with the NRC Headquarters Operations Center as soon as possible.

(i) Licensees must establish the requested continuous communications channel once the licensee has completed other required notifications under this section, § 50.72 of this chapter, appendix E to part 50 of this chapter, § 70.50 of this chapter; or § 72.75 of this chapter; as appropriate.

(ii) Licensees must complete any immediate actions required to stabilize the plant, to place the plant in a safe condition, to implement defensive measures, or to request assistance from the LLEA.

(iii) When established, the continuous communications channel must be staffed by a knowledgeable individual in the licensee's security, operations, or emergency response organizations from a location deemed appropriate by the licensee.

(iv) The continuous communications channel may be established via any available telephone system.

(6) For events reported under paragraph (b) of this section, the NRC may request that the licensee or its movement control center establish and maintain an open and continuous communications channel with the NRC Headquarters Operations Center as soon as possible.

(i) Licensees must establish the requested continuous communications channel once the licensee or the movement control center has completed other required notifications under this section, § 50.72 of this chapter, appendix E to part 50 of this chapter, or § 70.50 of this chapter; § 72.75 of this chapter; or requested assistance from the LLEA, as appropriate.

(ii) When established, the continuous communications channel must be staffed by a knowledgeable individual in the licensee's security, operations, or emergency response organizations or the movement control center monitoring the shipment.

(iii) The continuous communications channel may be established via any available telephone system.

(7)(i) For events reported under paragraphs (c), (e), (g), and (m) of this section, the NRC may request that the licensee establish and maintain an open and continuous communications channel with the NRC Headquarters Operations Center.

(ii) When established, the continuous communications channel must be staffed by a knowledgeable individual in the licensee's security, operations, or emergency response organizations from a location deemed appropriate by the licensee.

(iii) The continuous communications channel may be established via any available telephone system.

(8)(i) For events reported under paragraphs (d), (f), and (h) of this section, the NRC may request that the licensee or the movement control center establish and maintain an open and continuous communications channel with the NRC Headquarters Operations Center.

(ii) When established, the continuous communications channel must be staffed by a knowledgeable individual in the movement control center monitoring the shipment.

(iii) The continuous communications channel may be established via any available telephone system.

(p) *Significant supplemental information.* Licensees identifying significant supplemental information for events reported under paragraphs (a) through

(h), (m), and (n) of this section, subsequent to the initial telephonic notification to the NRC Headquarters Operations Center, must notify the NRC Headquarters Operations Center of such supplemental information under paragraph (o) of this section.

(q) *Retraction of previous security event reports.* (1) Licensees desiring to retract a previous physical security event notification made under paragraphs (a) through (h), (m), and (n) of this section, which have been determined to be invalid, not reportable in accordance with the requirements of paragraphs (a) through (h), (m), and (n) of this section, or recharacterized as recordable under §73.1210 of this part (instead of reportable under §73.1200), must telephonically notify the NRC Headquarters Operations Center in accordance with paragraph (o) of this section and indicate the report that is being retracted and the basis for the retraction.

(2) Invalid, not reportable, or recharacterized events include, but are not limited to, events for which the licensee subsequently receives new information regarding the event or relevant information from an external entity (*e.g.*, the initial information on a reportable event is subsequently determined to be incorrect or a law enforcement determination is made on the absence of a malevolent intent).

(r) *Declaration of emergencies.* Licensees notifying the NRC of the declaration of an emergency class must do so in accordance with §§50.72, 63.73, 70.50, and 72.75 of this chapter, as applicable.

(s) *Elimination of duplication.* Licensees with notification obligations under paragraphs (a) through (h), (m), and (n) of this section and §§50.72, 63.73, 70.50, and 72.75 of this chapter may notify the NRC of events in a single communication. This communication must identify each regulation under which the licensee is reporting.

(t) *Classified information.* Licensee notifications regarding security events associated with the deliberate disclosure, theft, loss, compromise, or possible compromise of classified documents, information, or material must comply with the requirements found in §95.57 of this chapter.

§73.1205 Written follow-up reports of physical security events.

(a) *General requirements.* (1) Licensees making a telephonic notification under §73.1200 of this part must also submit a written follow-up report to the NRC within 60 days of such notifications, in accordance with §73.4.

(2) As an exemption, licensees are not required to submit a written follow-up report subsequent to a telephonic notification made—

(i) Under the provisions of §73.1200(e) and (f) regarding interactions with a Federal, State, or local law-enforcement agency;

(ii) Under the provisions of §73.1200(m) regarding lost or stolen enhanced weapons; or

(iii) Under the provisions of §73.1200(n) regarding adverse findings from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) for enhanced weapons possessed by the licensee.

(3)(i) Licensees are not required to submit a written follow-up report if the licensee subsequently retracts a telephonic notification made under §73.1200 as invalid, not reportable under §73.1200, or recharacterized as recordable under §73.1210 (instead of reportable under §73.1200), and has not yet submitted a written follow-up report under this section.

(ii) If the licensee subsequently retracts a telephonic notification made under §73.1200 after it has submitted a written follow-up report under this section, then the licensee must submit a revised written follow-up report documenting the retraction.

(b) *Submission criteria.* (1) Each licensee must submit to the NRC written follow-up reports that contain sufficient information for NRC analysis and evaluation and are of a quality that will permit legible reproduction and processing.

(2)(i) Licensees subject to §50.73 of this chapter must prepare the written follow-up report on NRC Form 366.

(ii) Licensees not subject to §50.73 of this chapter must prepare the written follow-up report in a letter format.

(3)(i) If significant supplemental information becomes available after the submission of the initial written follow-up report, then the licensee must

submit a revised report with the revisions indicated.

(ii) The revised written follow-up report must replace the previous written report in its entirety. The update must be complete and not be limited to only supplementary or revised information.

(iii) Errors discovered in a written follow-up report must be corrected in a revised report with the revisions indicated.

(c) *Contents.* A written follow-up report must contain:

(1) A brief abstract describing the major occurrences during the event or condition, including all component or system failures that contributed to the event or condition, and significant corrective actions taken or planned to prevent recurrence.

(2) A clear, specific, narrative description of what occurred so that a knowledgeable reader conversant with general security program requirements, but not familiar with the security requirements for the specific facility or activity, can understand the complete event.

(3) The narrative description must include, as a minimum, the following information, as applicable—

(i) The date and time the event or condition was discovered;

(ii) The date and time the event or condition occurred;

(iii) The affected structures, systems, components, equipment, or procedures;

(iv) The environmental conditions at the time of the event or occurrence, if relevant;

(v) The root cause of the event or condition;

(vi) Whether any human performance errors were the cause or were a contributing factor to the event or condition, including: personnel errors, inadequate procedures, or inadequate training;

(vii) Whether previous events or conditions are relevant to the current event or condition and whether corrective actions to prevent recurrence were ineffective or insufficient;

(viii) Whether this event or condition is a recurring failure of a structure, system, component, or procedure important to security;

(ix) What compensatory measures, if any, were implemented in response to the event or condition;

(x) What corrective actions, if any, were taken in response to the event or condition; and

(xi) When corrective actions, if any, were taken or will be completed.

(d) *Transmission criteria.* (1) In addition to the addressees specified in § 73.4, the licensee must also provide one copy of the written follow-up report addressed to the Director, Office of Nuclear Security and Incident Response (NSIR).

(2) For copies of a classified written follow-up report, the licensee must transmit them to the NRC via either the NRC Headquarters classified mailing address specified in Table 2 of appendix A to this part or via the NRC's secure email address specified in Table 1 of appendix A to this part.

(3) Each written follow-up report containing classified information must be created, stored, marked, labeled, handled, transmitted to the NRC, and destroyed in accordance with the requirements of part 95 of this chapter.

(4) Each written follow-up report containing Safeguards Information must be created, stored, marked, labeled, handled, transmitted to the NRC, and destroyed in accordance with the requirements of §§ 73.21 and 73.22.

(e) *Records retention.* Licensees must maintain a copy of a written follow-up report as a record for a period of 3 years from the date of the report or until termination of the license, whichever is later.

§ 73.1210 Recordkeeping of physical security events.

(a) *Objective and purpose.* (1) Licensees with facilities or shipment activities subject to the provisions of § 73.20, § 73.25, § 73.26, § 73.27, § 73.37, § 73.45, § 73.46, § 73.50, § 73.51, § 73.55, § 73.60, or § 73.67, must record the physical security events and conditions adverse to security that are specified in paragraphs (c) through (f) of this section.

(2) These records facilitate the licensee's monitoring of the effectiveness of its physical security program. These records also facilitate the licensee's effective tracking, trending, and

performance monitoring of these security events and conditions adverse to security; and the subsequent identification and implementation of corrective actions to prevent recurrence.

(3) These physical security events and conditions adverse to security include, but are not limited to, human performance security errors; failure to comply with security procedures; insufficient or inadequate security procedures; security equipment failures and malfunctions; security structures, systems, and components design deficiencies; and inadequate or insufficient security structures, systems, and components. This includes events or conditions where the licensee has implemented compensatory measures within the required timeframe specified in its physical security plan.

(b) *General requirements.* (1) Licensees must record within 24 hours of the time of discovery the physical security events and conditions adverse to security specified in paragraphs (c) through (f) of this section.

(2) Licensees must retain these records for a period up to 3 years after the last entry is recorded, or until their license is terminated, whichever is later.

(3)(i) Licensees must record these physical security events and conditions adverse to security in either a standalone safeguards event log or as part of the licensee's corrective action program, as specified under the applicable quality assurance program provisions of parts 50, 52, 60, 63, 70, and 72 of this chapter, or both.

(ii) Licensees choosing to use their corrective action program to record these physical security events and conditions adverse to security must ensure that the records contain sufficient information to permit the effective tracking, trending, and performance monitoring of these events and conditions and the implementation of corrective actions.

(iii) Licensees must ensure that Safeguards Information or classified security information associated with these records is created, stored, and handled in accordance with the provisions of § 73.21, or of part 95 of this chapter, as applicable.

(iv) Licensees choosing to use their corrective action program for these records may also choose to bifurcate the information in such records systems so as to maximize the use and advantages of their corrective action programs' tracking, trending, and performance monitoring capabilities while simultaneously compartmenting sensitive security information and security vulnerabilities (*i.e.*, by controlling access and limiting need to know to necessary personnel), in order to ensure information protection requirements are effectively implemented.

(4) These records must include, but are not limited to, information on the following data elements, as applicable—

(i) The date and time the event or condition was discovered;

(ii) The date and time the event or condition occurred;

(iii) The affected structures, systems, components, equipment, or procedures;

(iv) A description of the event or condition;

(v) The environmental conditions at the time of the event or occurrence, if relevant;

(vi) The root cause of the event or condition;

(vii) Whether any human performance errors were the cause or were a contributing factor of the event or condition, including: personnel errors, inadequate procedures, or inadequate training;

(viii) Whether previous events or conditions are relevant to the current event or condition and whether corrective actions were ineffective or insufficient;

(ix) Whether this event or condition is a recurring failure of a structure, system, component, or procedure;

(x) What compensatory measures, if any, were implemented in response to the event or condition;

(xi) What corrective actions, if any, were taken in response to the event or condition; and

(xii) When corrective actions, if any, were taken or will be completed.

(5) Physical security events and conditions adverse to security for which notifications were made to the NRC under § 73.1200 are not required to be recorded under this section.

(6) Suspicious activities that are reported under § 73.1215 are not required to be recorded under this section.

(7) Enhanced weapons events that are reported under § 73.1200 are not required to be recorded under this section.

(c) *Compensated security events.* The requirements of this section apply to any failure, degradation, or discovered vulnerability in a security or safeguards system for which compensatory measures were established within the required timeframe and for which the following could have resulted in—

(1) Undetected access of unauthorized explosives beyond a required vehicle barrier;

(2) Unauthorized personnel gaining access into a protected area (PA), vital area (VA), material access area (MAA), or controlled access area (CAA);

(3) Undetected access of contraband into a PA, VA, or MAA;

(4) Unauthorized personnel accessing a vehicle transporting a Category I or II quantity of strategic special nuclear material (SSNM), spent nuclear fuel (SNF), or high-level radioactive waste (HLW);

(5) Unauthorized personnel accessing a Category I or II quantity of SSNM, SNF, or HLW being transported;

(6) Undetected introduction of contraband into a vehicle transporting a Category I or II quantity of SSNM, SNF, or HLW; or

(7) Undetected introduction of contraband into the Category I or II quantity of SSNM, SNF, or HLW being transported.

(d) *Ammunition events.* (1) For licensees with armed security personnel, the discovery that greater than a small quantity of live ammunition authorized by the licensee's security plan:

(i) Has been lost inside a PA, VA, or MAA; or

(ii) Has been found uncontrolled inside a PA, VA, or MAA.

(2)(i) The discovery that greater than a small quantity of unauthorized live ammunition is inside a PA, VA, or MAA.

(ii) A small quantity of live ammunition means five rounds or fewer of ammunition.

(iii) Uncontrolled authorized ammunition means ammunition authorized by the licensee's security plans that is not in the possession of authorized personnel or is not in an authorized ammunition storage location.

(iv) Unauthorized ammunition means ammunition that is not authorized by the licensee's security plans.

(3) As exemptions, licensees are not required to record:

(i) Ammunition that is in the possession of Federal, State, or local law-enforcement personnel performing official duties inside a PA, VA, or MAA is considered controlled and authorized; or

(ii) Blank ammunition used for training purposes by the licensee.

(e) [Reserved]

(f) *Decreases in the effectiveness of the physical security program.* The requirements of this section apply to any other threatened, attempted, or committed act not previously defined in this section that has resulted in or has the potential for decreasing the effectiveness of the licensee's physical security program below that committed to in a licensee's NRC-approved physical security plan.

(g) *Classified Information.* Licensee recordkeeping requirements regarding any security events or conditions adverse to security involving any infractions, losses, compromises, or possible compromise of classified information or classified documents are found in § 95.57 of this chapter.

(h) *Recordkeeping—exemptions.* Licensees subject to § 73.67 who possess or transport SSNM or special nuclear material (SNM) in the following categories are exempt from the provisions of this section:

(1) Category III quantity of SSNM;

(2) Category II quantity of SNM; or

(3) Category III quantity of SNM.

§ 73.1215 Suspicious activity reports.

(a) *Purpose.* This section sets forth the reporting criteria and process for licensees to use in reporting suspicious activities. Licensees are required to report suspicious activities to the local law enforcement agency (LLEA), the Federal Bureau of Investigation (FBI) local field office, the NRC, and the Federal Aviation Administration (FAA) local control tower if aircraft are a part of the suspicious activity.

(b) *Objective.* (1) A licensee's timely submission of suspicious activity reports (SARs) to Federal and local law enforcement agencies is an important part of the U.S. government's efforts to disrupt or dissuade malevolent acts against the nation's critical infrastructure. Despite the increasingly fluid and unpredictable nature of the threat environment, some elements of terrorist tactics, techniques, and procedures remain constant. For example, attack planning and preparation generally proceed through several predictable stages, including intelligence gathering and preattack surveillance or reconnaissance. These preattack stages, in particular, offer law enforcement and security personnel a significant opportunity to identify and disrupt or dissuade acts of terrorism before they occur. However, to use this information most effectively, timely reporting of suspicious activities by licensees to both Federal and local law enforcement is of vital importance.

(2) Licensee's timely submission of SARs to the NRC supports one of the agency's primary mission essential functions of threat assessment for licensed facilities, materials, and shipping activities.

(c) *General requirements.* (1)(i) Licensees subject to paragraphs (d), (e), and (f) of this section must report suspicious activities that are applicable to their facility, material, or shipping activity.

(ii) If a suspicious activity requires a physical security event notification pursuant to §73.1200, then the licensee is not required to also report the occurrence as a suspicious activity pursuant to this section.

(iii) If a suspicious activity report results in a LLEA response the licensee must notify the NRC in accordance with the requirements of §73.1200.

(2)(i) Licensees must promptly assess whether an activity is suspicious. Licensees may review additional information as part of an assessment process, including interactions with their LLEA. However, such assessments and any subsequent reporting must be completed as soon as possible, but within 4 hours of the time of discovery. The licensee must base its assessment upon its best available information on the activity, which may include its knowledge of its locale and the local population.

(ii) The licensee's assessment of a potential suspicious activity, and any discussion of this activity with its LLEA, does not constitute a conclusion, in and of itself, that the activity is suspicious.

(iii) Licensees are not required to report activities that, based on their assessment, appear to be innocent or innocuous.

(3) For a suspicious activity specified under paragraph (d) of this section, the licensee must make the following reports:

(i) First, to their LLEA;

(ii) Second, to their applicable FBI local field office;

(iii) Third, to the NRC Headquarters Operations Center; and

(iv) Lastly, to the local FAA control tower if the suspicious activity involves aircraft overflights in proximity to the licensee's facility.

(4) For a suspicious activity specified under paragraphs (e) and (f) of this section, the licensee or its designated movement control center must make the following reports, in the order indicated:

(i) First, to the applicable LLEA;

(ii) Second, to the applicable FBI local field office; and

(iii) Lastly, to the NRC Headquarters Operations Center.

(iv) For licensees making such reports related to shipping activities, the licensee responsible for the security of the shipment must contact the applicable FBI local field office.

(v) For a movement control center making such reports related to shipping activities, the applicable FBI local field office is as requested by the FBI. As such, the FBI may direct the use of the FBI local field office applicable to the movement control center itself or to the FBI local field office applicable to the licensee responsible for the security of the shipment.

(5)(i) Licensees subject to paragraphs (d) and (f) of this section must establish a point of contact with their local FBI field office.

(ii) Licensees subject to paragraph (d) of this section must establish a

point of contact with their local FAA control tower.

(6)(i) For licensees subject to paragraph (e) of this section who are responsible for the security of the shipment(s), the licensee must establish a point of contact with their local FBI field office.

(ii) For licensees subject to paragraph (e) of this section who are employing the services of a movement control center, the movement control center must establish a point of contact with its local FBI field office.

(7) Licensees and movement control centers reporting suspicious activities to the NRC must notify the NRC Headquarters Operations Center via the telephone number specified in Table 1 of appendix A of this part.

(8)(i) Licensees and movement control centers reporting suspicious activities must document the LLEA and FBI points of contact in written security communication procedures or route approvals, as applicable.

(ii) Licensees reporting suspicious aircraft overflight activities must document the FAA point of contact in written communication procedures.

(d) *Suspicious activities—facilities and materials.* (1) For licensees subject to the provisions of §73.20, §73.45, §73.46, §73.50, §73.51, §73.55, §73.60, or §73.67, the licensees must report activities they assess are suspicious. Examples include, but are not limited to, the following:

(i) Challenges to the licensee's security systems and procedures;

(ii) Elicitation of non-public information from knowledgeable licensee or contractor personnel regarding the licensee's security or emergency response programs;

(iii) Observed surveillance or reconnaissance activity from within posted or restricted areas (*i.e.*, non-public areas), including surface activity, underwater activity, manned aerial activity, and unmanned aerial activity;

(iv) Observed surveillance activity from public spaces outside of the licensee's control; or

(v) Unauthorized aircraft activities in close proximity to the facility (*i.e.*, above or near), involving either manned or unmanned aircraft, operating in a manner potentially indicative of surveillance or reconnaissance activity.

(2) As an exemption, this paragraph does not apply to:

(i) Licensees who are subject to the provisions of §73.67, and who are also engaged in the enrichment of special nuclear material using Restricted Data (RD) information, technology, or materials.

(ii) Licensees who are subject to the provisions of §73.67 of this part, and who are also engaged in the fabrication of new fuel assemblies.

(3) Licensees are not required to report commercial or military aircraft activity that is assessed as routine or non-threatening.

(e) *Suspicious activity—shipping activities.* (1) For licensees subject to the provisions of §73.20, §73.25, §73.26, §73.27, or §73.37, the licensee must report activities they assess are suspicious. Examples include, but are not limited to, the following:

(i) Challenges to the licensee's or its transportation contractor's communications subsystems regarding the transport system;

(ii) Challenges to the licensee's or its transportation contractor's security subsystems for the transport system;

(iii) Interference with or harassment of in-progress shipments;

(iv) Elicitation of non-public information from knowledgeable licensee personnel or the licensee's transportation contractor personnel regarding transportation program elements, including: security programs, operations programs, communication protocols, shipment routes, safe haven locations, and emergency response programs; or

(v) Observed surveillance or reconnaissance activity of ongoing shipments.

(2) For licensees using a movement control center for shipments of radioactive material or special nuclear material (SNM), the movement control center may report suspicious activities to LLEA, the FBI, and the NRC, in lieu of the licensee making such reports.

(f) *Suspicious activities—enrichment facilities.* (1) For licensees subject to the provisions of §73.67, who are also engaged in the enrichment of SNM using

RD information, technology, or materials; the licensee must report activities they assess are suspicious. Examples include, but are not limited to, the following:

(i) Aggressive noncompliance by visitors to the licensee's facility involving willful unauthorized departure from a tour group or willful unauthorized entry into restricted areas;

(ii) Unauthorized recording or imaging of sensitive technology, equipment, or materials; or

(iii) Elicitation of non-public information from knowledgeable licensee or contractor personnel regarding physical or information security programs intended to protect RD information, technology, or materials.

(2)(i) Licensees must report, in accordance with §95.57 of this chapter, alleged or suspected activities involving actual, attempted, or conspiracies to obtain RD, communicate RD, remove RD, or disclose RD in potential violation of Sections 224, 225, 226, and 227 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2274, 2275, 2276, and 2277).

(ii) As an exemption, the licensee is not required to also report such actual, attempted, or conspiracies to obtain RD, communicate RD, remove RD, or disclose RD as suspicious activities pursuant to this section.

(g) *Suspicious activities—exemptions.* (1) Licensees subject to §73.67 who possess strategic special nuclear material in quantities greater than 15 grams but less than the quantity necessary to form a critical mass, as specified in §150.11(a) of this chapter, are exempt from the provisions of this section.

(2) The following licensees are exempt from the provisions of this section:

(i) Docket number 70–7020; and

(ii) Docket number 70–7028.

APPENDIX A TO PART 73—U.S. NUCLEAR REGULATORY COMMISSION OFFICES AND CLASSIFIED MAILING ADDRESSES

TABLE 1—MAILING ADDRESSES, TELEPHONE NUMBERS, AND EMAIL ADDRESSES

	Address	Telephone (24-hour)	Email
NRC Headquarters Operations Center.	USNRC, Division of Preparedness and Response, Washington, DC 20555–0001.	(301) 816–5100; (301) 816–5151 (fax).	*Hoo.Hoc@nrc.gov; Hoo1@nrc.sgov.gov* (secure).
Region I: Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, and Vermont.	USNRC, Region I, 475 Allendale Road, Suite 102, King of Prussia, PA 19406–1415.	(610) 337–5000, (800) 432–1156 TDD: (301) 415–5575.	*RidsRgn1MailCenter@nrc.gov.*
Region II: Alabama, Florida, Georgia, Kentucky, North Carolina, Puerto Rico, South Carolina, Tennessee, Virginia, Virgin Islands, and West Virginia	USNRC, Region II, 245 Peachtree Center Avenue, NE., Suite 1200, Atlanta, GA 30303–1257.	(404) 997–4000, (800) 877–8510, TDD: (301) 415–5575.	*RidsRgn2MailC Center@nrc.gov*
Region III: Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, Ohio and Wisconsin	USNRC, Region III, 2443 Warrenville Road, Suite 210, Lisle, IL 60532–4352.	(630) 829–9500, (800) 522–3025, TDD: (301) 415–5575.	*RidsRgn3MailCenter@nrc.gov*

TABLE 1—MAILING ADDRESSES, TELEPHONE NUMBERS, AND EMAIL ADDRESSES—Continued

	Address	Telephone (24-hour)	Email
Region IV: Alaska, Arizona, Arkansas, California, Colorado, Hawaii, Idaho, Kansas, Louisiana, Mississippi, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Texas, Utah, Washington, Wyoming, and the U.S. territories and possessions in the Pacific.	US NRC, Region IV, 1600 E Lamar Blvd., Arlington, TX 76011–4511.	(817) 200–1100, (800) 952–9677, TDD: (301) 415–5575.	*RidsRgn4MailCenter@nrc.gov.*

TABLE 2—CLASSIFIED MAILING ADDRESSES
CLASSIFIED MAILING ADDRESSES

	Address
NRC Headquarters	U.S. NRC, Caller Box 2500, Rockville, MD 20852.
Region I	U.S. NRC, 475 Allendale Road, Suite 102, King of Prussia, PA 19406–1415.
Region II	USNRC, P.O. Box 56267, Atlanta, GA 30343.
Region III	USNRC, Region III, 2443 Warrenville Road, Suite 210, Lisle, IL 60532–4352.
Region IV	US NRC, Region IV, 1600 E. Lamar Blvd., Arlington, TX 76011–4511.

I. Classified mail shall be transmitted in accordance with §95.39 of this chapter to the appropriate NRC classified mailing address listed in this appendix.

II. Classified documents may be hand delivered to the NRC to the appropriate NRC street address listed in this appendix. Hand delivered classified documents shall be transmitted in accordance with §95.39 of this chapter.

III. Classified telephone calls must be made to the telephone numbers for the NRC Headquarters Operations Center in Table 1 of this appendix and the caller must request transfer to a secure telephone to communicate the classified information.

IV. Classified emails must be sent to the secure email address specified in Table 1 of this appendix.

[68 FR 58820, Oct. 10, 2003, as amended at 71 FR 15012, Mar. 27, 2006; 73 FR 30460, May 28, 2008; 75 FR 21981, Apr. 27, 2010; 76 FR 72086, Nov. 22, 2011; 77 FR 39909, July 6, 2012; 79 FR 66606, Nov. 10, 2014; 82 FR 52825, Nov. 15, 2017; 87 FR 20698, Apr. 8, 2022; 87 FR 68032, Nov. 14, 2022; 88 FR 15898, Mar. 14, 2023]

APPENDIX B TO PART 73—GENERAL CRITERIA FOR SECURITY PERSONNEL

TABLE OF CONTENTS

INTRODUCTION

Applicants and power reactor licensees subject to the requirements of §73.55 shall comply only with the requirements of section VI of this appendix. All other licensees, applicants, or certificate holders shall comply only with sections I through V of this appendix.

Security personnel who are responsible for the protection of special nuclear material on site or in transit and for the protection of the facility or shipment vehicle against radiological sabotage should, like other elements of the physical security system, be required to meet minimum criteria to ensure that they will effectively perform their assigned security-related job duties. In order to ensure that those individuals responsible for security are properly equipped and qualified to execute the job duties prescribed for them, the NRC has developed general criteria that specify security personnel qualification requirements.

These general criteria establish requirements for the selection, training, equipping, testing, and qualification of individuals who will be responsible for protecting special nuclear materials, nuclear facilities, and nuclear shipments.

When required to have security personnel that have been trained, equipped, and qualified to perform assigned security job duties in accordance with the criteria in this appendix, the licensee must establish, maintain, and follow a plan that shows how the criteria will be met. The plan must be submitted to the NRC for approval and must be implemented within 30 days after approval by the NRC unless otherwise specified by the NRC in writing.

DEFINITIONS

Terms defined in parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix.

CRITERIA

A. Employment Suitability and Qualification.

1. Suitability.

(a) Before employment, or assignment to the security organization, an individual shall:

(1) Possess a high school diploma or pass an equivalent performance examination designed to measure basic mathematical, language, and reasoning skills, abilities, and knowledge required to perform security duties and responsibilities;

(2) Have attained the age of 21 for an armed capacity or the age of 18 for an unarmed capacity;

(3) Not have any felony convictions that reflect on the individual's reliability; and

(4) Not be disqualified, in accordance with applicable state or Federal law from possessing or using firearms or ammunition.

(i) Licensees may use the information that has been obtained during the completion of the individual's background investigation for unescorted access to determine suitability; or

(ii) Licensees may use the satisfactory completion of a firearms background check for the individual under §73.17 of this part to also fulfill this requirement.

(b) The qualification of each individual to perform assigned duties and responsibilities must be documented by a qualified training instructor and attested to by a security supervisor.

B. Physical and mental qualifications. 1. Physical qualifications:

a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall have no physical weaknesses or abnormalities that would adversely affect their performance of assigned security job duties.

b. In addition to a. above, guards, armed response personnel, armed escorts, and central alarm station operators shall successfully pass a physical examination administered by a licensed physician. The examination shall be designed to measure the individual's physical ability to perform assigned security job duties as identified in the licensee physical security and contingency plans. Armed personnel shall meet the following additional physical requirements:

(1) Vision: (a) For each individual, distant visual acuity in each eye shall be correctable to 20/30 (Snellen or equivalent) in the better eye and 20/40 in the other eye with eyeglasses or contact lenses. If uncorrected distance vision is not at least 20/40 in the better eye, the individual shall carry an extra pair of corrective lenses. Near visual acuity, corrected or uncorrected, shall be at least 20/40 in the better eye. Field of vision must be at least 70° horizontal meridian in each eye. The ability

to distinguish red, green, and yellow colors is required. Loss of vision in one eye is disqualifying. Glaucoma shall be disqualifying, unless controlled by acceptable medical or surgical means, provided such medications as may be used for controlling glaucoma do not cause undesirable side effects which adversely affect the individual's ability to perform assigned security job duties, and provided the visual acuity and field of vision requirements stated above are met. On-the-job evaluation shall be used for individuals who exhibit a mild color vision defect.

(b) Where corrective eyeglasses are required, they shall be of the safety glass type.

(c) The use of corrective eyeglasses or contact lenses shall not interfere with an individual's ability to effectively perform assigned security job duties during normal or emergency operations.

(2) Hearing: (a) Individuals shall have no hearing loss in the better ear greater than 30 decibels average at 500 Hz, 1,000 Hz, and 2,000 Hz with no level greater that 40 decibels at any one frequency (by ISO 389 ''Standard Reference Zero for the Calibration of Puritone Audiometer'' (1975) or ANSI S3.6–1969 (R. 1973) ''Specifications for Audiometers''). ISO 389 and ANSI S3.6–1969 have been approved for incorporation by reference by the Director of the Federal Register. A copy of each standard is available for inspection at the NRC Library, 11545 Rockville Pike, Rockville, Maryland 20852-2738.

(b) A hearing aid is acceptable provided suitable testing procedures demonstrate auditory acuity equivalent to the above stated requirement.

(c) The use of a hearing aid shall not decrease the effective performance of the individual's assigned security job duties during normal or emergency operations.

(3) Diseases—Individuals shall have no established medical history or medical diagnosis of epilepsy or diabetes, or, where such a condition exists, the individual shall provide medical evidence that the condition can be controlled with proper medication so that the individual will not lapse into a coma or unconscious state while performing assigned security job duties.

(4) Addiction—Individuals shall have no established medical history or medical diagnosis of habitual alcoholism or drug addiction, or, where such a condition has existed, the individual shall provide certified documentation of having completed a rehabilitation program which would give a reasonable degree of confidence that the individual would be capable of performing assigned security job duties.

(5) Other physical requirements—An individual who has been incapacitated due to a serious illness, injury, disease, or operation, which could interfere with the effective performance of assigned security job duties shall, prior to resumption of such duties, provide medical evidence of recovery and ability to perform such security job duties.

2. Mental qualifications: a. Individuals whose security tasks and job duties are directly associated with the effective implementation of the licensee physical security and contingency plans shall demonstrate mental alertness and the capability to exercise good judgment, implement instructions, assimilate assigned security tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned job duties.

b. Armed individuals, and central alarm station operators, in addition to meeting the requirement stated in paragraph a. above, shall have no emotional instability that would interfere with the effective performance of assigned security job duties. The determination shall be made by a licensed psychologist or psychiatrist, or physician, or other person professionally trained to identify emotional instability.

c. The licensee shall arrange for continued observation of security personnel and for appropriate corrective measures by responsible supervisors for indications of emotional instability of individuals in the course of performing assigned security job duties. Identification of emotional instability by responsible supervisors shall be subject to verification by a licensed, trained person.

C. Medical examinations and physical fitness qualifications—Guards, armed response personnel, armed escorts and other armed security force members shall be given a medical examination including a determination and written certification by a licensed physician that there are no medical contraindications as disclosed by the medical examination to participation by the individual in physical fitness tests. Subsequent to this medical examination, guards, armed response personnel, armed escorts and other armed security force members shall demonstrate physical fitness for assigned security job duties by performing a practical physical exercise program within a specific time period. The exercise program performance objectives shall be described in the license training and qualifications plan and shall consider job-related functions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security job duties for both normal and emergency operations. The physical fitness qualification of each guard, armed response person, armed escort, and other security force member shall be documented and attested to by a licensee security supervisor. The licensee shall retain this documentation as a record for three years from the date of each qualification.

D. Contract security personnel—Contract security personnel shall be required to meet the suitability, physical, and mental requirements as appropriate to their assigned security job duties in accordance with section I of this appendix.

E. Physical requalification—At least every 12 months, central alarm station operators shall be required to meet the physical requirements of B.1.b of this section, and guards, armed response personnel, and armed escorts shall be required to meet the physical requirements of paragraphs B.1.b (1) and (2), and C of this section. The licensee shall document each individual's physical requalification and shall retain this documentation of requalification as a record for three years from the date of each requalification.

F. Documentation—The results of suitability, physical, and mental qualifications data and test results must be documented by the licensee or the licensee's agent. The licensee or the agent shall retain this documentation as a record for three years from the date of obtaining and recording these results.

G. Nothing herein authorizes or requires a licensee to investigate into or judge the reading habits, political or religious beliefs, or attitudes on social, economic, or political issues of any person.

II. Training and qualifications.

A. Training requirements—Each individual who requires training to perform assigned security-related job tasks or job duties as identified in the licensee physical security or contingency plans shall, prior to assignment, be trained to perform these tasks and duties in accordance with the licensee or the licensee's agent's documented training and qualifications plan. The licensee or the agent shall maintain documentation of the current plan and retain this documentation of the plan as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the plan was developed and, if any portion of the plan is superseded, retain the material that is superseded for three years after each change.

B. Qualification requirements—Each person who performs security-related job tasks or job duties required to implement the licensee physical security or contingency plan shall, prior to being assigned to these tasks or duties, be qualified in accordance with the licensee's NRC-approved training and qualifications plan. The qualifications of each individual must be documented and attested by a licensee security supervisor. The licensee shall retain this documentation of each individual's qualifications as a record for three years after the employee ends employment in the security-related capacity and for three years after the close of period for which the licensee possesses the special nuclear material under each license, and superseded material for three years after each change.

C. Contract personnel—Contract personnel shall be trained, equipped, and qualified as appropriate to their assigned security-related job tasks or job duties, in accordance with sections II, III, IV, and V of this appendix. The qualifications of each individual must be documented and attested by a licensee security supervisor. The licensee shall retain this documentation of each individual's qualifications as a record for three years after the employee ends employment in the security-related capacity and for three years after the close of period for which the licensee possesses the special nuclear material under each license, and superseded material for three years after each change.

D. Security knowledge, skills, and abilities—Each individual assigned to perform the security related task identified in the licensee physical security or contingency plan shall demonstrate the required knowledge, skill, and ability in accordance with the specified standards for each task as stated in the NRC approved licensee training and qualifications plan. The areas of knowledge, skills, and abilities that shall be considered in the licensee's training and qualifications plan are as follows:

1. Protection of nuclear facilities, transport vehicles, and special nuclear material.

2. NRC requirements and guidance for physical security at nuclear facilities and for transportation.

3. The private security guard's role in providing physical protection for the nuclear industry.

4. The authority of private guards.

5. The use of nonlethal weapons.

6. The use of deadly force.

7. Power of arrest and authority to detain individuals.

8. Authority to search individuals and seize property.

9. Adversary group operations.

10. Motivation and objectives of adversary groups.

11. Tactics and force that might be used by adversary groups to achieve their objectives.

12. Recognition of sabotage related devices and equipment that might be used against the licensee's facility or shipment vehicle.

13. Facility security organization and operation.

14. Types of physical barriers.

15. Weapons, lock and key control system operation.

16. Location of SNM and/or vital areas within a facility.

17. Protected area security and vulnerability.

18. Types of alarm systems used.

19. Response and assessment to alarm annunciations and other indications of intrusion.

20. Familiarization with types of special nuclear material processed.
21. General concepts of fixed site security systems.
22. Vulnerabilities and consequences of theft of special nuclear material or radiological sabotage of a facility.
23. Protection of security system information.
24. Personal equipment use and operation for normal and contingency operations.
25. Surveillance and assessment systems and techniques.
26. Communications systems operation, fixed site.
27. Access control systems and operation for individuals, packages, and vehicles.
28. Contraband detection systems and techniques.
29. Barriers and other delay systems around material access or vital areas.
30. Exterior and interior alarm systems operation.
31. Duress alarm operation.
32. Alarm stations operation.
33. Response force organization.
34. Response force mission.
35. Response force operation.
36. Response force engagement.
37. Security command and control system during normal operation.
38. Security command and control system during contingency operation.
39. Transportation systems security organization and operation.
40. Types of SNM transport vehicles.
41. Types of SNM escort vehicles.
42. Modes of transportation for SNM.
43. Road transport security system command and control structure.
44. Use of weapons.
45. Communications systems operation for transportation, shipment to control center and intraconvoy.
46. Vulnerabilities and consequences of theft of special nuclear material or radiological sabotage of a transport vehicle.
47. Protection of transport system security information.
48. Control of area around transport vehicle.
49. Normal convoy techniques and operations.
50. Familiarization with types of special nuclear materials shipped.
51. Fixed post station operations.
52. Access control system operation.
53. Search techniques and systems for individuals, packages and vehicles.
54. Escort and patrol responsibilities and operation.
55. Contengency response to confirmed intrusion or attempted intrusion.
56. Security system operation after component failure.
57. Fixed site security information protection.
58. Security coordination with local law enforcement agencies.
59. Security and situation reporting, documentation and report writing.
60. Contingency duties.
61. Self defense.
62. Use of and defenses against incapacitating agents.
63. Security equipment testing.
64. Contingency procedures.
65. Night vision devices and systems.
66. Mechanics of detention.
67. Basic armed and unarmed defensive tactics.
68. Response force deployment.
69. Security alert procedures.
70. Security briefing procedures.
71. Response force tactical movement.
72. Response force withdrawal.
73. Reponse force use of support fire.
74. Response to bomb and attack threats.
75. Response to civil disturbances (e.g., strikes, demonstrators).
76. Response to confirmed attempted theft of special nuclear material and/or radiological sabotage of facilities.
77. Response to hostage situations.
78. Site specific armed tactical procedures and operation.
79. Security response to emergency situations other than security incidents.
80. Basic transportation defensive response tactics.
81. Armed escort deployment.
82. Armed escort adversary engagement.
83. Armed escort formations.
84. Armed escort use of weapons fire (tactical and combat).
85. Armed escort and shipment movement under fire.
86. Tactical convoying techniques and operations.
87. Armed escort tactical exercises.
88. Armed escort response to bomb and attack threats.
89. Verification of shipment documentation and contents.
90. Continuous surveillance of shipment vehicle.
91. Normal and contingency operation for shipment mode transfer.
92. Armed personnel procedures and operation during temporary storage between mode transfers of shipments.
93. Armed escort threat assessment and response.
94. System for and operation of shipment vehicle lock and key control.
95. Techniques and procedures for isolation of shipment vehicle during a contingency situation.
96. Transportation coordination with local law enforcement agencies.
97. Procedures for verification of shipment locks and seals.

98. Transportation security and situation reporting, documentation, and report writing.

99. Procedures for shipment delivery and pickup.

100. Transportation security system for escort by road, rail, air and sea.

E. Requalification—Security personnel shall be requalified at least every 12 months to perform assigned security-related job tasks and duties for both normal and contingency operations. Requalification shall be in accordance with the NRC-approved licensee training and qualifications plan. The results of requalification must be documented and attested by a licensee security supervisor. The licensee shall retain this documentation of each individual's requalification as a record for three years from the date of each requalification.

III. Weapons training.

A. Guards, armed response personnel and armed escorts requiring weapons training to perform assigned security related job tasks or job duties shall be trained in accordance with the licensees' documented weapons training programs. Each individual shall be proficient in the use of his assigned weapon(s) and shall meet prescribed standards in the following areas:

1. Mechanical assembly, dissasembly, range penetration capability of weapon, and bullseye firing.

2. Weapons cleaning and storage.

3. Combat firing, day and night.

4. Safe weapons handling.

5. Clearing, loading, unloading, and reloading.

6. When to draw and point a weapon.

7. Rapid fire techniques.

8. Close quarter firing.

9. Stress firing.

10. Zeroing assigned weapon(s).

IV. Weapons qualification and requalification program.

Qualification firing for the handgun and the rifle must be for daylight firing, and each individual shall perform night firing for familiarization with assigned weapon(s). The results of weapons qualification and requalification must be documented by the licensee or the licensee's agent. Each individual shall be requalified at least every 12 months. The licensee shall retain this documentation of each qualification and requalification as a record for three years from the date of the qualification or requalification, as appropriate.

A. Handgun—Guards, armed escorts and armed response personnel shall qualify with a revolver or semiautomatic pistol firing the national police course, or an equivalent nationally recognized course. Qualifying score shall be an accumulated total of 70 percent of the maximum obtainable score.

B. Semiautomatic Rifle—Guards, armed escorts and armed response personnel, assigned to use the semiautomatic rifle by the licensee training and qualifications plan, shall qualify with a semiautomatic rifle by firing the 100-yard course of fire specified in section 17.5(1) of the National Rifle Association, High Power Rifle Rules book (effective March 15, 1976),[1] or a nationally recognized equivalent course of fire. Targets used shall be as stated in section 17.5 for the 100-yard course. Time limits for individuals shall be as specified in section 8.2 of the NRA rule book, regardless of the course fired. Qualifying score shall be an accumulated total of 80 percent of the maximum obtainable score.

C. Shotgun—Guards, armed escorts, and armed response personnel assigned to use the 12 gauge shotgun by the licensee training and qualifications plan shall qualify with a full choke or improved modified choke 12 gauge shotgun firing the following course:

Range	Position	No. Rounds[1]	Target[2]
15 yds	Hip fire point	4	B–27
25 yds	Shoulder	4	B–27

[1] The 4 rounds shall be fired at 4 separate targets within 10 seconds using 00 gauge (9 pellet) shotgun shells.

[2] As set forth by the National Rifle Association (NRA) in its official rules and regulations, ''NRA Target Manufacturers Index,'' December 1976. The Index has been approved for incorporation by reference by the Director of the Federal Register. A copy of the index is available for inspection at the NRC Library, 11545 Rockville Pike, Rockville, Maryland 20852-2738.

To qualify the individual shall be required to place 50 percent of all pellets (36 pellets) within the black silhouette.

D. Requalification—Individuals shall be weapons requalified at least every 12 months in accordance with the NRC approved licensee training and qualifications plan, and in accordance with the requirements stated in A, B, and C of this section.

V. Guard, armed response personnel, and armed escort equipment.

A. Fixed Site—Fixed site guards and armed response personnel shall either be equipped with or have available the following security equipment appropriate to the individual's assigned contingency security related tasks or job duties as described in the licensee physical security and contingency plans:

1. Semiautomatic rifles with following nominal minimum specifications:

(a) .223 caliber.

(b) Muzzle velocity, 1980 ft/sec.

(c) Muzzle energy, 955 foot-pounds.

(d) Magazine or clip load of 10 rounds.

(e) Magazine reload, <10 seconds.

[1] Copies of the ''NRA High Power Rifle Rules'' may be examined at, or obtained from, the National Rifle Association, 1600 Rhode Island Avenue NW., Washington, DC 20036.

(f) Operable in any environment in which it will be used.

2. 12 gauge shotguns with the following capabilities:

(a) 4 round pump or semiautomatic.

(b) Operable in any environment in which it will be used.

(c) Full or modified choke.

3. Semiautomatic pistols or revolvers with the following nominal minimum specifications:

(a) .354 caliber.

(b) Muzzle energy, 250 foot-pounds.

(c) Full magazine or cylinder reload capability <6 seconds.

(d) Muzzle velocity, 850 ft/sec.

(e) Full cylinder or magazine capacity, 6 rounds.

(f) Operable in any environment in which it will be used.

4. Ammunition:

(a) For each assigned weapon as appropriate to the individual's assigned contingency security job duties and as readily available as the weapon:

(1) 18 rounds per handgun.

(2) 100 rounds per semiautomatic rifle.

(3) 12 rounds each per shotgun (00 gauge and slug).

(b) Ammunition available on site—two (2) times the amount stated in (a) above for each weapon.

5. Personal equipment to be readily available for individuals whose assigned contingency security job duties, as described in the licensee physical security and contingency plans, warrant such equipment:

(a) Helmet, combat.

(b) Gas mask, full face.

(c) Body armor (bullet-resistant vest).

(d) Flashlights and batteries.

(e) Baton.

(f) Handcuffs.

(g) Ammunition/equipment belt.

6. Binoculars.

7. Night vision aids, *i.e.*, hand-fired illumination flares or equivalent.

8. Tear gas or other nonlethal gas.

9. Duress alarms.

10. Two-way portable radios (handi-talkie) 2 channels minimum, 1 operating and 1 emergency.

B. Transportation—Armed escorts shall either be equipped with or have readily available the following security equipment appropriate to the individual's assigned contingency security related tasks or job duties, as described in the licensee physical security and contingency plans:

1. Semiautomatic rifles with the following nominal minimum specifications:

(a) .223 caliber.

(b) Muzzle velocity, 1,980 ft/sec.

(c) Muzzle energy, 955 foot-pounds.

(d) Magazine or clip of 10 rounds.

(e) Reload capability, 10 seconds.

(f) Operable in any environment in which it will be used.

2. 12 gauge shotguns.

(a) 4 round pump or semiautomatic.

(b) Operable in any environment in which it will be used.

(c) Full or modified choke.

3. Semiautomatic pistols or revolvers with the following nominal minimum specifications:

(a) .354 caliber.

(b) Muzzle energy, 250 foot-pounds.

(c) Full magazine or cylinder reload capability 6 seconds.

(d) Muzzle velocity, 850 ft/sec.

(e) Full cylinder or magazine capacity, 6 rounds.

(f) Operable in any environment in which it will be used.

4. Ammunition for each shipment.

(a) For each assigned weapon as appropriate to the individual's assigned contingency security job duties and as readily available as the weapon:

(1) 36 rounds per handgun.

(2) 120 rounds per semiautomatic rifle.

(3) 12 rounds each per shotgun (00 gauge and slug).

5. Escort vehicles, bullet resisting, equipped with communications systems, red flares, first aid kit, emergency tool kit, tire changing equipment, battery chargers for radios (where appropriate, for recharging portable radio batteries).

6. Personal equipment to be readily available for individuals whose assigned contingency security job duties, as described in the licensee physical security and contingency plans, warrant such equipment:

(a) Helmet, combat.

(b) Gas mask, full face.

(c) Body armor (bullet-resistant vest).

(d) Flashlights and batteries.

(e) Baton.

(f) Ammunition/equipment belt.

(g) Pager/duress alarms.

7. Binoculars.

8. Night vision aids, *i.e.*, hand-fired illumination flares or equivalent.

9. Tear gas or other nonlethal gas.

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

A. General Requirements and Introduction

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

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

3. The licensee shall establish, maintain, and follow a Commission-approved training and qualification plan, describing how the minimum training and qualification requirements set forth in this appendix will be met, to include the processes by which all individuals, will be selected, trained, equipped, tested, and qualified.

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

5. The licensee shall ensure that the training and qualification program simulates, as closely as practicable, the specific conditions under which the individual shall be required to perform assigned duties and responsibilities.

6. The licensee may not allow any individual to perform any security function, assume any security duties or responsibilities, or return to security duty, until that individual satisfies the training and qualification requirements of this appendix and the Commission-approved training and qualification plan, unless specifically authorized by the Commission.

7. Annual requirements must be scheduled at a nominal twelve (12) month periodicity. Annual requirements may be completed up to three (3) months before or three (3) months after the scheduled date. However, the next annual training must be scheduled twelve (12) months from the previously scheduled date rather than the date the training was actually completed.

B. Employment Suitability and Qualification

1. Suitability.

(a) Before employment, or assignment to the security organization, an individual shall:

(1) Possess a high school diploma or pass an equivalent performance examination designed to measure basic mathematical, language, and reasoning skills, abilities, and knowledge required to perform security duties and responsibilities;

(2) Have attained the age of 21 for an armed capacity or the age of 18 for an unarmed capacity; and

(3) Not have any felony convictions that reflect on the individual's reliability.

(4) Individuals in an armed capacity, would not be disqualified from possessing or using firearms or ammunition in accordance with applicable state or Federal law, to include 18 U.S.C. 922. Licensees shall use information that has been obtained during the completion of the individual's background investigation for unescorted access to determine suitability.

(b) The qualification of each individual to perform assigned duties and responsibilities must be documented by a qualified training instructor and attested to by a security supervisor.

2. Physical qualifications.

(a) General physical qualifications.

(1) Individuals whose duties and responsibilities are directly associated with the effective implementation of the Commission-approved security plans, licensee protective strategy, and implementing procedures, may not have any physical conditions that would adversely affect their performance of assigned security duties and responsibilities.

(2) Armed and unarmed individuals assigned security duties and responsibilities shall be subject to a physical examination designed to measure the individual's physical ability to perform assigned duties and responsibilities as identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(3) This physical examination must be administered by a licensed health professional with the final determination being made by a licensed physician to verify the individual's physical capability to perform assigned duties and responsibilities.

(4) The licensee shall ensure that both armed and unarmed individuals who are assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures, meet the following minimum physical requirements, as required to effectively perform their assigned duties.

(b) Vision.

(1) For each individual, distant visual acuity in each eye shall be correctable to 20/30 (Snellen or equivalent) in the better eye and 20/40 in the other eye with eyeglasses or contact lenses.

(2) Near visual acuity, corrected or uncorrected, shall be at least 20/40 in the better eye.

(3) Field of vision must be at least 70 degrees horizontal meridian in each eye.

(4) The ability to distinguish red, green, and yellow colors is required.

(5) Loss of vision in one eye is disqualifying.

(6) Glaucoma is disqualifying, unless controlled by acceptable medical or surgical means, provided that medications used for controlling glaucoma do not cause undesirable side effects which adversely affect the individual's ability to perform assigned security duties, and provided the visual acuity and field of vision requirements stated previously are met.

(7) On-the-job evaluation must be used for individuals who exhibit a mild color vision defect.

(8) If uncorrected distance vision is not at least 20/40 in the better eye, the individual shall carry an extra pair of corrective lenses in the event that the primaries are damaged. Corrective eyeglasses must be of the safety glass type.

(9) The use of corrective eyeglasses or contact lenses may not interfere with an individual's ability to effectively perform assigned duties and responsibilities during normal or emergency conditions.

(c) Hearing.

(1) Individuals may not have hearing loss in the better ear greater than 30 decibels average at 500 Hz, 1,000 Hz, and 2,000 Hz with no level greater than 40 decibels at any one frequency.

(2) A hearing aid is acceptable provided suitable testing procedures demonstrate auditory acuity equivalent to the hearing requirement.

(3) The use of a hearing aid may not decrease the effective performance of the individual's assigned security duties during normal or emergency operations.

(d) Existing medical conditions.

(1) Individuals may not have an established medical history or medical diagnosis of existing medical conditions which could interfere with or prevent the individual from effectively performing assigned duties and responsibilities.

(2) If a medical condition exists, the individual shall provide medical evidence that the condition can be controlled with medical treatment in a manner which does not adversely affect the individual's fitness-for-duty, mental alertness, physical condition, or capability to otherwise effectively perform assigned duties and responsibilities.

(e) Addiction. Individuals may not have any established medical history or medical diagnosis of habitual alcoholism or drug addiction, or, where this type of condition has existed, the individual shall provide certified documentation of having completed a rehabilitation program which would give a reasonable degree of confidence that the individual would be capable of effectively performing assigned duties and responsibilities.

(f) Other physical requirements. An individual who has been incapacitated due to a serious illness, injury, disease, or operation, which could interfere with the effective performance of assigned duties and responsibilities shall, before resumption of assigned duties and responsibilities, provide medical evidence of recovery and ability to perform these duties and responsibilities.

3. Psychological qualifications.

(a) Armed and unarmed individuals shall demonstrate the ability to apply good judgment, mental alertness, the capability to implement instructions and assigned tasks, and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned duties and responsibilities.

(b) A licensed psychologist, psychiatrist, or physician trained in part to identify emotional instability shall determine whether armed members of the security organization and alarm station operators in addition to meeting the requirement stated in paragraph (a) of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

(c) A person professionally trained to identify emotional instability shall determine whether unarmed individuals in addition to meeting the requirement stated in paragraph (a) of this section, have no emotional instability that would interfere with the effective performance of assigned duties and responsibilities.

4. Medical examinations and physical fitness qualifications.

(a) Armed members of the security organization shall be subject to a medical examination by a licensed physician, to determine the individual's fitness to participate in physical fitness tests.

(1) The licensee shall obtain and retain a written certification from the licensed physician that no medical conditions were disclosed by the medical examination that would preclude the individual's ability to participate in the physical fitness tests or meet the physical fitness attributes or objectives associated with assigned duties.

(b) Before assignment, armed members of the security organization shall demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test.

(1) The physical fitness test must consider physical conditions such as strenuous activity, physical exertion, levels of stress, and exposure to the elements as they pertain to each individual's assigned security duties for both normal and emergency operations and must simulate site specific conditions under which the individual will be required to perform assigned duties and responsibilities.

(2) The licensee shall describe the physical fitness test in the Commission-approved training and qualification plan.

(3) The physical fitness test must include physical attributes and performance objectives which demonstrate the strength, endurance, and agility, consistent with assigned duties in the Commission-approved security plans, licensee protective strategy, and implementing procedures during normal and emergency conditions.

(4) The physical fitness qualification of each armed member of the security organization must be documented by a qualified training instructor and attested to by a security supervisor.

5. Physical requalification.

(a) At least annually, armed and unarmed individuals shall be required to demonstrate the capability to meet the physical requirements of this appendix and the licensee training and qualification plan.

(b) The physical requalification of each armed and unarmed individual must be documented by a qualified training instructor and attested to by a security supervisor.

C. Duty Training

1. Duty training and qualification requirements. All personnel who are assigned to perform any security-related duty or responsibility shall be trained and qualified to perform assigned duties and responsibilities to ensure that each individual possesses the minimum knowledge, skills, and abilities required to effectively carry out those assigned duties and responsibilities.

(a) The areas of knowledge, skills, and abilities that are required to perform assigned duties and responsibilities must be identified in the licensee's Commission-approved training and qualification plan.

(b) Each individual who is assigned duties and responsibilities identified in the Commission-approved security plans, licensee protective strategy, and implementing procedures shall, before assignment:

(1) Be trained to perform assigned duties and responsibilities in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(2) Meet the minimum qualification requirements of this appendix and the Commission-approved training and qualification plan.

(3) Be trained and qualified in the use of all equipment or devices required to effectively perform all assigned duties and responsibilities.

2. On-the-job training.

(a) The licensee training and qualification program must include on-the-job training performance standards and criteria to ensure that each individual demonstrates the requisite knowledge, skills, and abilities needed to effectively carry-out assigned duties and responsibilities in accordance with the Commission-approved security plans, licensee protective strategy, and implementing procedures, before the individual is assigned the duty or responsibility.

(b) In addition to meeting the requirement stated in paragraph C.2.(a) of this appendix, before assignment, individuals (e.g., response team leaders, alarm station operators, armed responders, and armed security officers designated as a component of the protective strategy) assigned duties and responsibilities to implement the Safeguards Contingency Plan shall complete a minimum of 40 hours of on-the-job training to demonstrate their ability to effectively apply the knowledge, skills, and abilities required to effectively perform assigned *contingency* duties and responsibilities in accordance with the approved safeguards contingency plan, other security plans, licensee protective strategy, and implementing procedures. On-the-job training must be documented by a qualified training instructor and attested to by a security supervisor.

(c) On-the-job training for contingency activities and drills must include, but is not limited to, hands-on application of knowledge, skills, and abilities related to:

(1) Response team duties.

(2) Use of force.

(3) Tactical movement.

(4) Cover and concealment.

(5) Defensive positions.

(6) Fields-of-fire.

(7) Re-deployment.

(8) Communications (primary and alternate).

(9) Use of assigned equipment.

(10) Target sets.

(11) Table top drills.

(12) Command and control duties.

(13) Licensee Protective Strategy.

3. Performance Evaluation Program.

(a) Licensees shall develop, implement and maintain a Performance Evaluation Program that is documented in procedures which describes how the licensee will demonstrate and assess the effectiveness of their onsite physical protection program and protective strategy, including the capability of the armed response team to carry out their assigned duties and responsibilities during safeguards contingency events. The Performance Evaluation Program and procedures shall be referenced in the licensee's Training and Qualifications Plan.

(b) The Performance Evaluation Program shall include procedures for the conduct of tactical response drills and force-on-force exercises designed to demonstrate and assess the effectiveness of the licensee's physical protection program, protective strategy and contingency event response by all individuals with responsibilities for implementing the safeguards contingency plan.

(c) The licensee shall conduct tactical response drills and force-on-force exercises in

accordance with Commission-approved security plans, licensee protective strategy, and implementing procedures.

(d) Tactical response drills and force-on-force exercises must be designed to challenge the site protective strategy against elements of the design basis threat and ensure each participant assigned security duties and responsibilities identified in the Commission-approved security plans, the licensee protective strategy, and implementing procedures demonstrate the requisite knowledge, skills, and abilities.

(e) Tactical response drills, force-on-force exercises, and associated contingency response training shall be conducted under conditions that simulate, as closely as practicable, the site-specific conditions under which each member will, or may be, required to perform assigned duties and responsibilities.

(f) The scope of tactical response drills conducted for training purposes shall be determined by the licensee and must address site-specific, individual or programmatic elements, and may be limited to specific portions of the site protective strategy.

(g) Each tactical response drill and force-on-force exercise shall include a documented post-exercise critique in which participants identify failures, deficiencies or other findings in performance, plans, equipment or strategies.

(h) Licensees shall document scenarios and participants for all tactical response drills and annual force-on-force exercises conducted.

(i) Findings, deficiencies and failures identified during tactical response drills and force-on-force exercises that adversely affect or decrease the effectiveness of the protective strategy and physical protection program shall be entered into the licensee's corrective action program to ensure that timely corrections are made to the appropriate program areas.

(j) Findings, deficiencies and failures associated with the onsite physical protection program and protective strategy shall be protected as necessary in accordance with the requirements of 10 CFR 73.21.

(k) For the purpose of tactical response drills and force-on-force exercises, licensees shall:

(1) Use no more than the total number of armed responders and armed security officers documented in the security plans.

(2) Minimize the number and effects of artificialities associated with tactical response drills and force-on-force exercises.

(3) Implement the use of systems or methodologies that simulate the realities of armed engagement through visual and audible means, and reflect the capabilities of armed personnel to neutralize a target through the use of firearms.

(4) Ensure that each scenario used provides a credible, realistic challenge to the protective strategy and the capabilities of the security response organization.

(l) The Performance Evaluation Program must be designed to ensure that:

(1) Each member of each shift who is assigned duties and responsibilities required to implement the safeguards contingency plan and licensee protective strategy participates in at least one (1) tactical response drill on a quarterly basis and one (1) force-on-force exercise on an annual basis. Force-on-force exercises conducted to satisfy the NRC triennial evaluation requirement can be used to satisfy the annual force-on-force requirement for the personnel that participate in the capacity of the security response organization.

(2) The mock adversary force replicates, as closely as possible, adversary characteristics and capabilities of the design basis threat described in 10 CFR 73.1(a)(1), and is capable of exploiting and challenging the licensees protective strategy, personnel, command and control, and implementing procedures.

(3) Protective strategies can be evaluated and challenged through the conduct of tactical response tabletop demonstrations.

(4) Drill and exercise controllers are trained and qualified to ensure that each controller has the requisite knowledge and experience to control and evaluate exercises.

(5) Tactical response drills and force-on-force exercises are conducted safely and in accordance with site safety plans.

(m) Scenarios.

(1) Licensees shall develop and document multiple scenarios for use in conducting quarterly tactical response drills and annual force-on-force exercises.

(2) Licensee scenarios must be designed to test and challenge any components or combination of components, of the onsite physical protection program and protective strategy.

(3) Each scenario must use a unique target set or target sets, and varying combinations of adversary equipment, strategies, and tactics, to ensure that the combination of all scenarios challenges every component of the onsite physical protection program and protective strategy to include, but not limited to, equipment, implementing procedures, and personnel.

D. Duty Qualification and Requalification

1. Qualification demonstration.

(a) Armed and unarmed individuals shall demonstrate the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(b) This demonstration must include written exams and hands-on performance demonstrations.

(1) Written Exams. The written exams must include those elements listed in the Commission-approved training and qualification plan and shall require a minimum score of 80 percent to demonstrate an acceptable understanding of assigned duties and responsibilities, to include the recognition of potential tampering involving both safety and security equipment and systems.

(2) Hands-on Performance Demonstrations. Armed and unarmed individuals shall demonstrate hands-on performance for assigned duties and responsibilities by performing a practical hands-on demonstration for required tasks. The hands-on demonstration must ensure that theory and associated learning objectives for each required task are considered and each individual demonstrates the knowledge, skills, and abilities required to effectively perform the task.

(3) Annual Written Exam. Armed individuals shall be administered an annual written exam that demonstrates the required knowledge, skills, and abilities to carry out assigned duties and responsibilities as an armed member of the security organization. The annual written exam must include those elements listed in the Commission-approved training and qualification plan and shall require a minimum score of 80 percent to demonstrate an acceptable understanding of assigned duties and responsibilities.

(c) Upon request by an authorized representative of the Commission, any individual assigned to perform any security-related duty or responsibility shall demonstrate the required knowledge, skills, and abilities for each assigned duty and responsibility, as stated in the Commission-approved security plans, licensee protective strategy, or implementing procedures.

2. Requalification.

(a) Armed and unarmed individuals shall be requalified at least annually in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(b) The results of requalification must be documented by a qualified training instructor and attested by a security supervisor.

E. Weapons Training

1. General firearms training.

(a) Armed members of the security organization shall be trained and qualified in accordance with the requirements of this appendix and the Commission-approved training and qualification plan.

(b) Firearms instructors.

(1) Each armed member of the security organization shall be trained and qualified by a certified firearms instructor for the use and maintenance of each assigned weapon to include but not limited to, marksmanship, assembly, disassembly, cleaning, storage, handling, clearing, loading, unloading, and reloading, for each assigned weapon.

(2) Firearms instructors shall be certified from a national or state recognized entity.

(3) Certification must specify the weapon or weapon type(s) for which the instructor is qualified to teach.

(4) Firearms instructors shall be recertified in accordance with the standards recognized by the certifying national or state entity, but in no case shall recertification exceed three (3) years.

(c) Annual firearms familiarization. The licensee shall conduct annual firearms familiarization training in accordance with the Commission-approved training and qualification plan.

(d) The Commission-approved training and qualification plan shall include, but is not limited to, the following areas:

(1) Mechanical assembly, disassembly, weapons capabilities and fundamentals of marksmanship.

(2) Weapons cleaning and storage.

(3) Combat firing, day and night.

(4) Safe weapons handling.

(5) Clearing, loading, unloading, and reloading.

(6) Firing under stress.

(7) Zeroing duty weapon(s) and weapons sighting adjustments.

(8) Target identification and engagement.

(9) Weapon malfunctions.

(10) Cover and concealment.

(11) Weapon familiarization.

(e) The licensee shall ensure that each armed member of the security organization is instructed on the use of deadly force as authorized by applicable state law.

(f) Armed members of the security organization shall participate in weapons range activities on a nominal four (4) month periodicity. Performance may be conducted up to five (5) weeks before, to five (5) weeks after, the scheduled date. The next scheduled date must be four (4) months from the originally scheduled date.

F. Weapons Qualification and Requalification Program

1. General weapons qualification requirements.

(a) Qualification firing must be accomplished in accordance with Commission requirements and the Commission-approved training and qualification plan for assigned weapons.

(b) The results of weapons qualification and requalification must be documented and retained as a record.

2. Tactical weapons qualification. The licensee Training and Qualification Plan must describe the firearms used, the firearms qualification program, and other tactical

training required to implement the Commission-approved security plans, licensee protective strategy, and implementing procedures. Licensee developed tactical qualification and re-qualification courses must describe the performance criteria needed to include the site specific conditions (such as lighting, elevation, fields-of-fire) under which assigned personnel shall be required to carry-out their assigned duties.

3. Firearms qualification courses. The licensee shall conduct the following qualification courses for each weapon used.

(a) Annual daylight qualification course. Qualifying score must be an accumulated total of 70 percent with handgun and shotgun, and 80 percent with semiautomatic rifle and/or enhanced weapons, of the maximum obtainable target score.

(b) Annual night fire qualification course. Qualifying score must be an accumulated total of 70 percent with handgun and shotgun, and 80 percent with semiautomatic rifle and/or enhanced weapons, of the maximum obtainable target score.

(c) Annual tactical qualification course. Qualifying score must be an accumulated total of 80 percent of the maximum obtainable score.

4. Courses of fire.

(a) Handgun. Armed members of the security organization, assigned duties and responsibilities involving the use of a revolver or semiautomatic pistol shall qualify in accordance with standards established by a law enforcement course, or an equivalent nationally recognized course.

(b) Semiautomatic rifle. Armed members of the security organization, assigned duties and responsibilities involving the use of a semiautomatic rifle shall qualify in accordance with the standards established by a law enforcement course, or an equivalent nationally recognized course.

(c) Shotgun. Armed members of the security organization, assigned duties and responsibilities involving the use of a shotgun shall qualify in accordance with standards established by a law enforcement course, or an equivalent nationally recognized course.

(d) Enhanced weapons. Armed members of the security organization, assigned duties and responsibilities involving the use of any weapon or weapons not described previously shall qualify in accordance with applicable standards established by a law enforcement course or an equivalent nationally recognized course for these weapons.

5. Firearms requalification.

(a) Armed members of the security organization shall be re-qualified for each assigned weapon at least annually in accordance with Commission requirements and the Commission-approved training and qualification plan, and the results documented and retained as a record.

(b) Firearms requalification must be conducted using the courses of fire outlined in paragraphs F.2, F.3, and F.4 of this section.

G. Weapons, Personal Equipment and Maintenance

1. Weapons. The licensee shall provide armed personnel with weapons that are capable of performing the function stated in the Commission-approved security plans, licensee protective strategy, and implementing procedures.

2. Personal equipment.

(a) The licensee shall ensure that each individual is equipped or has ready access to all personal equipment or devices required for the effective implementation of the Commission-approved security plans, licensee protective strategy, and implementing procedures.

(b) The licensee shall provide armed security personnel, required for the effective implementation of the Commission-approved Safeguards Contingency Plan and implementing procedures, at a minimum, but is not limited to, the following:

(1) Gas mask, full face.

(2) Body armor (bullet-resistant vest).

(3) Ammunition/equipment belt.

(4) Two-way portable radios, 2 channels minimum, 1 operating and 1 emergency.

(c) Based upon the licensee protective strategy and the specific duties and responsibilities assigned to each individual, the licensee should provide, as appropriate, but is not limited to, the following.

(1) Flashlights and batteries.

(2) Baton or other non-lethal weapons.

(3) Handcuffs.

(4) Binoculars.

(5) Night vision aids (e.g., goggles, weapons sights).

(6) Hand-fired illumination flares or equivalent.

(7) Duress alarms.

3. Maintenance.

(a) Firearms maintenance program. Each licensee shall implement a firearms maintenance and accountability program in accordance with the Commission regulations and the Commission-approved training and qualification plan. The program must include:

(1) Semiannual test firing for accuracy and functionality.

(2) Firearms maintenance procedures that include cleaning schedules and cleaning requirements.

(3) Program activity documentation.

(4) Control and accountability (weapons and ammunition).

(5) Firearm storage requirements.

(6) Armorer certification.

H. Records

1. The licensee shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of §73.55(q).

2. The licensee shall retain each individual's initial qualification record for three (3) years after termination of the individual's employment and shall retain each re-qualification record for three (3) years after it is superseded.

3. The licensee shall document data and test results from each individual's suitability, physical, and psychological qualification and shall retain this documentation as a record for three (3) years from the date of obtaining and recording these results.

I. Reviews

The licensee shall review the Commission-approved training and qualification program in accordance with the requirements of §73.55(m).

J. Definitions

Terms defined in parts 50, 70, and 73 of this chapter have the same meaning when used in this appendix.

[43 FR 37426, Aug. 23, 1978, as amended at 46 FR 2026, Jan. 8, 1981; 53 FR 405, Jan. 7, 1988; 53 FR 19261, May 27, 1988; 57 FR 33432, July 29, 1992; 57 FR 61787, Dec. 29, 1992; 59 FR 50689, Oct. 5, 1994; 74 FR 13987, Mar. 27, 2009; 77 FR 39910, July 6, 2012; 84 FR 63569, Nov. 18, 2019; 88 FR 15898, Mar. 14, 2023]

APPENDIX C TO PART 73—LICENSEE SAFEGUARDS CONTINGENCY PLANS

I. SAFEGUARDS CONTINGENCY PLAN

Licensees, applicants, and certificate holders, with the exception of those who are subject to the requirements of §73.55 shall comply with the requirements of this section.

INTRODUCTION

A licensee safeguards contingency plan is a documented plan to give guidance to licensee personnel in order to accomplish specific defined objectives in the event of threats, thefts, or radiological sabotage relating to special nuclear material or nuclear facilities licensed under the Atomic Energy Act of 1954, as amended. An acceptable safeguards contingency plan must contain:

(1) A predetermined set of decisions and actions to satisfy stated objectives;

(2) An identification of the data, criteria, procedures, and mechanisms necessary to efficiently implement the decisions; and

(3) A stipulation of the individual, group, or organizational entity responsible for each decision and action.

The goals of licensee safeguards contingency plans for responding to threats, thefts, and radiological sabotage are:

(1) To organize the response effort at the licensee level;

(2) To provide predetermined, structured responses by licensees to safeguards contingencies;

(3) To ensure the integration of the licensee response with the responses by other entities; and

(4) To achieve a measurable performance in response capability.

Licensee safeguards contingency planning should result in organizing the licensee's resources in such a way that the participants will be identified, their several responsibilities specified, and the responses coordinated. The responses should be timely.

It is important to note that a licensee's safeguards contingency plan is intended to be complementary to any emergency plans developed under appendix E to part 50 of this chapter, §52.17 or §52.79, or to §70.22(i) of this chapter.

CONTENTS OF THE PLAN

Each licensee safeguards contingency plan shall include five categories of information:

1. Background
2. Generic Planning Base
3. Licensee Planning Base
4. Responsibility Matrix
5. Procedures

Although the implementing procedures (the fifth category of Plan information) are the culmination of the planning process, and therefore are an integral and important part of the safeguards contingency plan, they entail operating details subject to frequent changes. They need not be submitted to the Commission for approval, but will be inspected by NRC staff on a periodic basis. The licensee is responsible for ensuring that the implementing procedures reflect the information in the Responsibility Matrix, appropriately summarized and suitably presented for effective use by the responding entities.

The following paragraphs describe the contents of the safeguards contingency plan.

1. *Background.* Under the following topics, this category of information shall identify and define the perceived dangers and incidents with which the plan will deal and the general way it will handle these:

a. Perceived Danger—A statement of the perceived danger to the security of special nuclear material, licensee personnel, and licensee property, including covert diversion of special nuclear material, radiological sabotage, and overt attacks. The statement of perceived danger should conform with that promulgated by the Nuclear Regulatory Commission. (The statement contained in 10 CFR 73.55(a) or subsequent Commission statements will suffice.)

b. Purpose of the Plan—A discussion of the general aims and operational concepts underlying implementation of the plan.

c. Scope of the Plan—A delineation of the types of incidents covered in the plan.

d. Definitions—A list of terms and their definitions used in describing operational and technical aspects of the plan.

2. *Generic Planning Base.* Under the following topics, this category of information shall define the criteria for initiation and termination of responses to safeguards contingencies together with the specific decisions, actions, and supporting information needed to bring about such responses:

a. Identification of those events that will be used for signaling the beginning or aggravation of a safeguards contingency according to how they are perceived initially by licensee's personnel. Such events may include alarms or other indications signaling penetration of a protected area, vital area, or material access area; material control or material accounting indications of material missing or unaccounted for; or threat indications—either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

b. Definition of the specific objective to be accomplished relative to each identified event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency in order to prepare for further responses; to establish a level of response preparedness; or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

3. *Licensee Planning Base.* This category of information shall include the factors affecting contingency planning that are specific for each facility or means of transportation. To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they may be incorporated by cross reference to that plan. The following topics should be addressed:

a. Licensee's Organizational Structure for Contingency Responses—A delineation of the organization's chain of command and delegation of authority as these apply to safeguards contingencies.

b. Physical Layout—(i) Fixed Sites—A description of the physical structures and their location on the site, and a description of the site in relation to nearby town, roads, and other environmental features important to the effective coordination of response operations. Particular emphasis should be placed on main and alternate entry routes for law-enforcement assistance forces and the location of control points for marshalling and coordinating response activities.

(ii) Transportation—A description of the vehicles, shipping routes, preplanned alternate routes, and related features.

c. Safeguards Systems Hardware—A description of the physical security and accounting system hardware that influence how the licensee will respond to an event. Examples of systems to be discussed are communications, alarms, locks, seals, area access, armaments, and surveillance.

d. Law Enforcement Assistance—A listing of available local law enforcement agencies and a description of their response capabilities and their criteria for response; and a discussion of working agreements or arrangements for communicating with these agencies.

e. Policy Constraints and Assumptions—A discussion of State laws, local ordinances, and company policies and practices that govern licensee response to incidents. Examples that may be discussed include:

Use of deadly force;
Use of employee property;
Use of off-duty employees;
Site security jurisdictional boundaries.

f. Administrative and Logistical Considerations—Descriptions of licensee practices that may have an influence on the response to safeguards contingency events. The considerations shall include a description of the procedures that will be used for ensuring that all equipment needed to effect a successful response to a safeguards contingency will be easily accessible, in good working order, and in sufficient supply to provide redundancy in case of equipment failure.

4. *Responsibility Matrix.* This category of information consists of detailed identification of the organizational entities responsible for each decision and action associated with specific responses to safeguards contingencies. For each initiating event, a tabulation shall be made for each response entity depicting the assignment of responsibilities for all decisions and actions to be taken in response to the initiating event. (Not all entities will have assigned responsibilities for any given initiating event.) The tabulations in the Responsibility Matrix shall provide an overall picture of the response actions and their interrelationships. Safeguards responsibilities shall be assigned in a manner that precludes conflict in duties or responsibilities that would prevent the execution of the plan in any safeguards contingency.

5. *Procedures.* In order to aid execution of the detailed plan as developed in the Responsibility Matrix, this category of information shall detail the actions to be taken and decisions to be made by each member or unit of the organization as planned in the Responsibility Matrix.

AUDIT AND REVIEW

(1) For nuclear facilities subject to the requirements of §73.46, the licensee shall provide for a review of the safeguards contingency plan at intervals not to exceed 12 months. For nuclear power reactor licensees subject to the requirements of §73.55, the licensee shall provide for a review of the safeguards contingency plan either:

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

(ii) 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 safeguards contingency plan must be reviewed at least every 24 months.

(2) A licensee subject to the requirements of either §73.46 or §73.55 shall ensure that the review of the safeguards contingency plan is by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program. The review must include an audit of safeguards contingency procedures and practices, and an audit of commitments established for response by local law enforcement authorities.

(3) The licensee shall document the results and the recommendations of the safeguards contingency plan review, management findings on whether the safeguards contingency plan is currently effective, and any actions taken as a result of recommendations from prior reviews 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. The report must be maintained in an auditable form, available for inspection for a period of 3 years.

II. Nuclear Power Plant Safeguards Contingency Plans

A. Introduction

The safeguards contingency plan is a documented plan that describes how licensee personnel implement their physical protection program to defend against threats to their facility, up to and including the design basis threat of radiological sabotage. The goals of licensee safeguards contingency plans are:

(1) To organize the response effort at the licensee level;

(2) To provide predetermined, structured response by licensees to safeguards contingencies;

(3) To ensure the integration of the licensee response by other entities; and

(4) To achieve a measurable performance in response capability.

Licensee safeguards contingency planning should result in organizing the licensee's resources in such a way that the participants will be identified, their responsibilities specified, and the responses coordinated. The responses should be timely, and include personnel who are trained and qualified to respond in accordance with a documented training and qualification program.

The evaluation, validation, and testing of this portion of the program shall be conducted in accordance with appendix B, section VI of this part, Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties. The licensee's safeguards contingency plan is intended to maintain effectiveness during the implementation of emergency plans developed under appendix E to part 50 of this chapter.

B. Contents of the Plan

Each safeguards contingency plan shall include five (5) categories of information:

(1) Background.

(2) Generic planning base.

(3) Licensee planning base.

(4) Responsibility matrix.

(5) Implementing procedures.

Although the implementing procedures (the fifth category of plan information) are the culmination of the planning process, and are an integral and important part of the safeguards contingency plan, they entail operating details subject to frequent changes. They need not be submitted to the Commission for approval, but are subject to inspection by NRC staff on a periodic basis.

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

a. Perceived Danger—Consistent with the design basis threat specified in §73.1(a)(1), licensees shall identify and describe the perceived dangers, threats, and incidents against which the safeguards contingency plan is designed to protect.

b. Purpose of the Plan—Licensees shall describe the general goals, objectives and operational concepts underlying the implementation of the approved safeguards contingency plan.

c. Scope of the Plan—A delineation of the types of incidents covered by the plan.

(i) How the onsite response effort is organized and coordinated to effectively respond to a safeguards contingency event.

(ii) How the onsite response for safeguards contingency events has been integrated in other site emergency response procedures.

d. Definitions—A list of terms and their definitions used in describing operational and technical aspects of the approved safeguards contingency plan.

2. Generic Planning Base. Licensees shall define the criteria for initiation and termination of responses to security events to include the specific decisions, actions, and supporting information needed to respond to each type of incident covered by the approved safeguards contingency plan. To achieve this result the generic planning base must:

a. Identify those events that will be used for signaling the beginning or aggravation of a safeguards contingency event according to how they are perceived initially by licensee's personnel. Licensees shall ensure detection of unauthorized activities and shall respond to all alarms or other indications signaling a

security event, such as penetration of a protected area, vital area, or unauthorized barrier penetration (vehicle or personnel); tampering, bomb threats, or other threat warnings—either verbal, such as telephoned threats, or implied, such as escalating civil disturbances.

b. Define the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses; to establish a level of response preparedness; or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

c. Identify the data, criteria, procedures, mechanisms and logistical support necessary to achieve the objectives identified.

3. Licensee Planning Base. This category of information shall include factors affecting safeguards contingency planning that are specific for each facility. To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they may be incorporated by reference in the Safeguards Contingency Plan. The following topics must be addressed:

a. Organizational Structure. The safeguards contingency plan must describe the organization's chain of command and delegation of authority during safeguards contingency events, to include a general description of how command and control functions will be coordinated and maintained.

b. Physical Layout. The safeguards contingency plan must include a site map depicting the physical structures located on the site, including onsite independent spent fuel storage installations, and a description of the structures depicted on the map. Plans must also include a description and map of the site in relation to nearby towns, transportation routes (e.g., rail, water, and roads), pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Descriptions and maps must indicate main and alternate entry routes for law enforcement or other offsite response and support agencies and the location for marshaling and coordinating response activities.

c. Safeguards Systems. The safeguards contingency plan must include a description of the physical security systems that support and influence how the licensee will respond to an event in accordance with the design basis threat described in §73.1(a). The licensee's description shall begin with onsite physical protection measures implemented at the outermost facility perimeter, and must move inward through those measures implemented to protect target set equipment.

(i) Physical security systems and security systems hardware to be discussed include security systems and measures that provide defense-in-depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

(ii) The specific structure of the security response organization to include the total number of armed responders and armed security officers documented in the approved security plans as a component of the protective strategy and a general description of response capabilities shall also be included in the safeguards contingency plan.

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

(iv) Armed responders shall be available to respond from designated areas inside the protected area at all times and may not be assigned any other duties or responsibilities that could interfere with assigned armed response team duties and responsibilities.

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

(1) Be designed to meet the performance requirements and objectives of §73.55(a) through (k).

(2) Identify predetermined actions, areas of responsibility and timelines for the deployment of armed personnel.

(3) Contain measures that limit the exposure of security personnel to possible attack, including incorporation of bullet resisting protected positions.

(4) Contain a description of the physical security systems and measures that provide defense-in-depth such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

(5) Describe the specific structure and responsibilities of the armed response organization to include:

The authorized minimum number of armed responders, available at all times inside the protected area.

The authorized minimum number of armed security officers, available onsite at all times.

The total number of armed responders and armed security officers documented in the

approved security plans as a component of the protective strategy.

(6) Provide a command and control structure, to include response by off-site law enforcement agencies, which ensures that decisions and actions are coordinated and communicated in a timely manner to facilitate response.

d. Law Enforcement Assistance. Provide a listing of available law enforcement agencies and a general description of their response capabilities and their criteria for response and a discussion of working agreements or arrangements for communicating with these agencies.

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

(i) Use of deadly force.

(ii) Recall of off-duty employees.

(iii) Site jurisdictional boundaries.

(iv) Use of enhanced weapons, if applicable.

f. Administrative and Logistical Considerations. Descriptions of licensee practices which influence how the security organization responds to a safeguards contingency event to include, but not limited to, a description of the procedures that will be used for ensuring that equipment needed to facilitate response will be readily accessible, in good working order, and in sufficient supply.

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

a. Licensees shall develop site procedures that consist of matrixes detailing the organization and/or personnel responsible for decisions and actions associated with specific responses to safeguards contingency events. The responsibility matrix and procedures shall be referenced in the licensee's safeguards contingency plan.

b. Responsibility matrix procedures shall be based on the events outlined in the licensee's Generic Planning Base and must include the following information:

(i) The definition of the specific objective to be accomplished relative to each identified safeguards contingency event. The objective may be to obtain a level of awareness about the nature and severity of the safeguards contingency to prepare for further responses, to establish a level of response preparedness, or to successfully nullify or reduce any adverse safeguards consequences arising from the contingency.

(ii) A tabulation for each identified initiating event and each response entity which depicts the assignment of responsibilities for decisions and actions to be taken in response to the initiating event.

(iii) An overall description of response actions and interrelationships specifically associated with each responsible entity must be included.

c. Responsibilities shall be assigned in a manner that precludes conflict of duties and responsibilities that would prevent the execution of the safeguards contingency plan and emergency response plans.

d. Licensees shall ensure that predetermined actions can be completed under the postulated conditions.

5. Implementing Procedures.

(i) Licensees shall establish and maintain written implementing procedures that provide specific guidance and operating details that identify the actions to be taken and decisions to be made by each member of the security organization who is assigned duties and responsibilities required for the effective implementation of the security plans and the site protective strategy.

(ii) Licensees shall ensure that implementing procedures accurately reflect the information contained in the Responsibility Matrix required by this appendix, the security plans, and other site plans.

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

C. Records and Reviews

1. Licensees shall review the safeguards contingency plan in accordance with the requirements of §73.55(m).

2. The safeguards contingency plan audit must include a review of applicable elements of the Physical Security Plan, Training and Qualification Plan, implementing procedures and practices, the site protective strategy, and response agreements made by local, State, and Federal law enforcement authorities.

3. Licensees shall retain all reports, records, or other documentation required by this appendix in accordance with the requirements of §73.55(q).

(Sec. 161i, Pub. L. 83–703, 68 Stat. 948, secs. 201, 204(b)(1), Pub L. 93–438, 88 Stat. 1243, 1245 (42 U.S.C. 2201, 5841, 5844))

[43 FR 11965, Mar. 23, 1978; 43 FR 14007, Apr. 4, 1978, as amended at 57 FR 33432, July 29, 1992; 64 FR 14818, Mar. 29, 1999; 72 FR 49562, Aug. 28, 2007; 74 FR 13991, Mar. 27, 2009; 77 FR 39910, July 6, 2012]

Appendix D to Part 73—Physical Protection of Irradiated Reactor Fuel in Transit, Training Program Subject Schedule

Pursuant to the provision of §73.37 of 10 CFR part 73, each licensee who transports or

delivers to a carrier for transport irradiated reactor fuel is required to assure that individuals used as shipment escorts have completed a training program. The subjects that are to be included in this training program are as follows:

Security Enroute

—Route planning and selection
—Vehicle operation
—Procedures at stops
—Detours and use of alternate routes

Communications

—Equipment operation
—Status reporting
—Contacts with law enforcement units
—Communications discipline
—Procedures for reporting incidents

Radiological Considerations

—Description of the radioactive cargo
—Function and characteristics of the shipping casks
—Radiation hazards
—Federal, State and local ordinances relative to the shipment of radioactive materials
—Responsible agencies

Response to Contingencies

—Accidents
—Severe weather conditions
—Vehicle breakdown
—Communications problems
—Radioactive ''spills''
—Use of special equipment (flares, emergency lighting, etc.)

Response to Threats

—Reporting
—Calling for assistance
—Use of immobilization features
—Hostage situations
—Avoiding suspicious situations

The licensee is also required to assure that armed individuals serving as shipment escorts, other than members of local law enforcement agencies, have completed a weapons training and qualifications program equivalent to that required of guards, as described in III and IV of appendix B of this part, to assure that each such individual is fully qualified to use weapons assigned him.

[44 FR 34468, June 15, 1979, as amended at 45 FR 34710, June 3, 1980]

APPENDIX E TO PART 73—LEVELS OF PHYSICAL PROTECTION TO BE APPLIED IN INTERNATIONAL TRANSPORT OF NUCLEAR MATERIAL[1]

(Verbatim from Annex I to the Convention on the Physical Protection of Nuclear Material)

(a) Levels of physical protection for nuclear material during storage incidental to international nuclear transport include:

(1) For Category III materials, storage within an area to which access is controlled;

(2) For Category II materials, storage within an area under constant surveillance by guards or electronic devices, surrounded by a physical barrier with a limited number of points of entry under appropriate control or any area with an equivalent level of physical protection;

(3) For Category I material, storage within a protected area as defined for Category II, to which, in addition, access is restricted to persons whose trustworthiness has been determined, and which is under surveillance by guards who are in close communication with appropriate response forces. Specific measures taken in this context should have as their objective the detection and prevention of any assault, unauthorized access, or unauthorized removal of material.

(b) Levels of physical protection for nuclear material during international transport include:

(1) For Category II and III materials, transportation shall take place under special precautions including prior arrangements among sender, receiver, and carrier, and prior agreement between natural or legal persons subject to the jurisdiction and regulation of exporting and importing States, specifying time, place and procedures for transferring transport responsibility;

(2) For Category I materials, transportation shall take place under special precautions identified for transportation of Category II and III materials, and in addition, under constant surveillance by escorts and under conditions which assure close communication with appropriate response forces;

(3) For natural uranium other than in the form of ore or ore residue, transportation

[1] See appendix C to part 110 of this chapter from the physical description of the categories of nuclear material as set forth in Annex I to the Convention. For the purposes of this part, the following categories of nuclear material are synonymous:

Category I is a formula quantity of strategic special nuclear material;

Category II is special nuclear material of moderate strategic significance or irradiated fuel; and

Category III is special nuclear material of low strategic significance.

protection for quantities exceeding 500 kilograms U shall include advance notification of shipment specifying mode of transport, expected time of arrival and [shall provide for] confirmation of receipt of shipment.

[52 FR 9654, Mar. 26, 1987]

APPENDIX F TO PART 73—COUNTRIES AND ORGANIZATIONS THAT ARE PARTIES TO THE CONVENTION ON THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL[1]

COUNTRIES/ORGANIZATIONS

Afghanistan
Albania
Algeria
Andorra
Antigua and Barbuda
Argentina
Armenia
Australia
Austria
Azerbaijan
Bahamas
Bahrain
Bangladesh
Belarus
Belgium
Bolivia
Bosnia and Herzegovina
Botswana
Brazil
Bulgaria
Burkina Faso
Cabo Verde
Cambodia
Cameroon
Canada
Central African Republic
Chile
China
Colombia
Comoros
Costa Rica
Côte d'Ivoire
Croatia
Cuba
Cyprus
Czech Republic
Democratic Rep. of the Congo
Denmark
Djibouti
Dominica
Dominican Republic
Ecuador
El Salvador
Equatorial Guinea
Estonia
Eswatini
Fiji
Finland
France
Gabon
Georgia
Germany
Ghana
Greece
Grenada
Guatemala
Guinea
Guinea-Bissau
Guyana
Haiti
Honduras
Hungary
Iceland
India
Indonesia
Iraq
Ireland
Israel
Italy
Jamaica
Japan
Jordan
Kazakhstan
Kenya
Korea, Republic of
Kuwait
Kyrgyzstan
Lao P.D.R.
Latvia
Lebanon
Lesotho
Libya
Liechtenstein
Lithuania
Luxembourg
Madagascar
Malawi
Mali
Malta
Marshall Islands
Mauritania
Mexico
Monaco
Mongolia
Montenegro
Morocco
Mozambique
Myanmar
Namibia
Nauru
Netherlands
New Zealand
Nicaragua
Niger
Nigeria
Niue
Norway
Oman

[1] An updated list of party countries and organizations will appear annually in the International Atomic Energy Agency's publication, Convention on the Physical Protection of Nuclear Material, at *https://www-legacy.iaea.org/Publications/Documents/Conventions/cppnm_status.pdf*. Appendix F will be amended as required to maintain its currency.

Pakistan
Palau
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Republic of Moldova
Romania
Russian Federation
Rwanda
Saint Kitts and Nevis
Saint Lucia
San Marino
Saudi Arabia
Senegal
Serbia
Seychelles
Singapore
Slovakia
Slovenia
South Africa
Spain
Sudan
Sweden
Switzerland
Tajikistan
Thailand
The frmr. Yug. Rep. of Macedonia
Togo
Tonga
Trinidad and Tobago
Tunisia
Turkey
Turkmenistan
Uganda
Ukraine
United Arab Emirates
United Kingdom
United Republic of Tanzania
United States of America
Uruguay
Uzbekistan
Viet Nam
Yemen
Zambia
EURATOM

[83 FR 58465, Nov. 20, 2018]

APPENDIX G TO PART 73 [RESERVED]

APPENDIX H TO PART 73—WEAPONS QUALIFICATION CRITERIA

The B–27 Target or a target of equivalent difficulty will be used for all weapon qualification testing.

TABLE H–1—MINIMUM DAY FIRING CRITERIA [1]

[see footnotes at end of Table H–1]

Weapon	Stage	String [2]	Distance	Number of rounds	Timing [3]	Position	Scoring
Handgun.	1	1 2 3	3 yards	6	9 seconds	Draw and fire 2 rounds (repeat 2 times) 3 seconds each string.	Minimum qualifying = 70%.
	2	1 2	7 yards	6	10 seconds	Draw and fire 2 rounds at center mass and 1 round at the head (repeat once) 5 seconds each string.	
	3	1 2 3	7 yards	6	12 seconds (4 seconds each string).	Using weaker hand only, from the low ready position, fire 2 rounds (repeat twice).	
	4	1	10 yards ...	2	4 seconds	Draw and fire 2 rounds, come to low ready position.	
		2	10 yards ...	2	3 seconds	Fire 2 rounds from low ready position and reholster.	
		3	10 yards ...	4	12 seconds (revolver) 10 seconds (semiautomatic).	Draw and fire 2 rounds, reload, fire 2 rounds and reholster.	
		4	10 yards ...	2	4 seconds	Draw and fire 2 rounds, come to low ready position.	
		5	10 yards ...	2	3 seconds	Fire 2 rounds from low ready position and reholster.	
	5	1	15 yards ...	2	5 seconds	Standing, draw weapon, move to kneeling position, then fire 2 rounds and reholster.	
		2	15 yards ...	2	5 seconds	Standing, draw weapon, move to kneeling position, then fire 2 rounds and reholster.	

TABLE H–1—MINIMUM DAY FIRING CRITERIA [1]—Continued

[see footnotes at end of Table H–1]

Weapon	Stage	String [2]	Distance	Number of rounds	Timing [3]	Position	Scoring
	5	3	15 yards ...	4	14 seconds (revolver) 12 seconds (semiautomatic).	Standing, draw weapon, fire 2 rounds, move to kneeling position and fire 2 rounds, reload and reholster.	Minimum qualifying = 70%.
		4	15 yards ...	2	5 seconds	Draw weapon and fire 2 rounds standing, come to low ready position and....	
		5	15 yards ...	2	3 seconds	Fire 2 rounds from low ready.	
	6	1	25 yards ...	2	5 seconds	Draw and fire 2 rounds, standing, left side of barricade.	
		2	25 yards ...	2	5 seconds	Draw and fire 2 rounds, right side of barricade (standing).	
		3	25 yards ...	4	15 seconds (revolver) 12 seconds (semi-automatic).	Draw weapon and move from standing to kneeling position, fire 2 rounds, left side of barricade, reload, and from the kneeling position, fire 2 rounds, right side of barricade.	
		4	25 yards ...	2	10 seconds	Draw weapon and move from standing to prone, fire 2 rounds.	
		5	25 yards ...	2	10 seconds	Draw weapon and move from standing to prone, fire 2 rounds.	
	7	1	50 yards ...	2	8 seconds	Draw weapon and fire 2 rounds from a standing barricade position (right or left side, shooter's option).	
		2	50 yards ...	2	10 seconds	Draw weapon and fire 2 rounds from a kneeling barricade position (right or left side, shooter's option).	
		3	50 yards ...	2	12 seconds	Draw weapon and fire 2 rounds from prone position.	
Shotgun	1	1	7 yards	2 Double 0 buckshot	4 seconds	At low ready position fire 2 rounds standing.	Minimum qualifying = 70%.
	2	1 2	15 yards ...	4 Double 0 buckshot	15 seconds	At low ready position fire 2 rounds standing, reload and fire 2 rounds.	
	3	1 2	25 yards ...	4 rifled slugs or 00 buckshot	20 seconds	On command, load 4 rounds and fire 2 rounds standing and 2 rounds kneeling.	
Rifle	1	1 2 3	15 yards ...	6	10 seconds (4 seconds for 1st string, 3 seconds for each of 2nd and 3rd string).	Standing in low ready position, move to standing point shoulder position (1 magazine loaded with 6 rounds, weapon in half-load configuration), fire 2 rounds per string.	Minimum qualifying = 70%.
	2	1 2 3	25 yards ...	6	11 seconds (5 seconds for 1st string, 3 seconds for each of 2nd and 3rd string).	Standing in low ready position, move to standing point shoulder position (1 magazine loaded with 6 rounds, weapon in half-load configuration), fire 2 rounds per string.	
	3	1 2 3	25 yards ...	6	17 seconds (7 seconds for 1st string, 5 seconds for each of 2nd and 3rd string).	Standing in low ready position, move to kneeling point shoulder position (1 magazine loaded with 6 rounds, weapon in half-load configuration), fire 2 rounds per string.	
	4	1 2	50 yards ...	4	16 seconds (9 seconds for 1st string, 7 second for 2nd string).	Standing in low ready position, move to kneeling point shoulder position (1 magazine loaded with 4 rounds, weapon in half-load configuration), fire 2 rounds per string.	

TABLE H–1—MINIMUM DAY FIRING CRITERIA [1]—Continued

[see footnotes at end of Table H–1]

Weapon	Stage	String [2]	Distance	Number of rounds	Timing [3]	Position	Scoring
	[4]5	1	50 yards ...	4	20 seconds	Standing in low ready position, move to prone (weapon in half-load configuration) with two magazines each loaded with 2 rounds, fire 2 rounds, reload with 2nd magazine and fire 2 rounds.	Minimum qualifying = 70%.
	[4]6	1	100 yards	4	25 seconds	Standing in low ready position, move to prone (weapon in half-load configuration) two magazines each loaded with 2 rounds, fire 2 rounds, reload with 2nd magazine and fire 2 rounds.	

Footnotes:
[1] This day firing qualifications course is to be used by all TRT members, armed response personnel, and guards.
[2] A string is one of the different phases within a single stage.
[3] Security personnel will be timed as shown.
[4] Stages 5 and 6 are to be used for .30 caliber or larger rifles.

TABLE H–2—MINIMUM NIGHT FIRING CRITERIA

Weapon	Stage	Distance	No. of rounds	Timing	Position	Scoring	Lighting
Handgun (Rev.).	1	7 yds	12	35 seconds	Standing-no artificial support.	Minimum qualifying = 70%.	For all courses 0.2 footcandles at center mass of target area.
	2	15 yds	12	45 seconds.			
Handgun (Semi-).	1	7 yds	2 + clip	30 seconds	Standing-no artificial support.		
	2	15 yds	2 + clip	40 seconds.			
Shotgun	1	25 yds	2 rifled slugs ..	30 seconds (Load 2 slugs—chamber empty—Time starts—Commence firing).	Standing-strong shoulder.	Rifled slug hits = strike area on target (10, 9, 7).	
	1	15 yds	5 Double 0 buckshot.	10 seconds (Load 5rds Buckshot—chamber, empty—Time starts—Commence firing).	Standing-strong shoulder.	Double 0 Buckshot: Hits in black = 2 pts (5rds × 9 pellets/rd × 2 pts = 90) Minimum qualifying = 70%.	
Rifle	1	25 yds	1–5rd mag	45 sec	Standing-barricade.	Minimum qualifying = 70%.	
	2	25 yds	1–5rd mag	45 sec	Standing.		
	3	25 yds	1–5rd mag	45 sec	Kneeling.		
	4	25 yds	1–5rd mag	45 sec	Prone.		

Note. All firing is to be done only at night. Use of night simulation equipment during daylight is not allowable. Use of site specific devices (*i.e.*, laser, etc.) should be included in the licensee amended security plan for NRC approval.

[58 FR 45785, Aug. 31, 1993]