

## § 73.22

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,

## 10 CFR Ch. I (1–1–23 Edition)

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 determina-

tion. 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 § 73.71 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 In-

formation 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]

### **§ 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: