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]

§ 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 related to panoramic and underwater irradiators that possess greater than 370 TBq (10,000 Ci) of byproduct material in the form of sealed sources; manufacturers and distributors of items containing source material, or byproduct or special nuclear material in greater than or equal to Category 2 quantities of concern; transportation of more than 1000 Tbq (27,000 Ci) but less than or equal to 100 grams of spent nuclear fuel; research and test reactors that possess special nuclear material of moderate strategic significance or special nuclear material of low strategic significance; and transportation of source, byproduct, or special nuclear material in greater than or equal to Category 1 quantities of concern. 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 more than 1000 Tbq (27,000 Ci) but less than or equal to 100 grams of spent nuclear fuel, source material and byproduct material in Category 1 quantities of concern, and 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 §73.71 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]

§ 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]

PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL IN TRANSIT

§ 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