Protection of Safeguards Information Requirements for Tribes Participating in the Advance Notification of Irradiated Reactor Fuel Shipments

General Requirement

Information and material that meets the criteria set forth in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.21, "Protection of Safeguards Information: Performance Requirements," must be protected from unauthorized disclosure. The U.S. Nuclear Regulatory Commission (NRC) has determined that the information contained in the advance notification for shipments of irradiated reactor fuel and certain nuclear wastes is designated as Safeguards Information (SGI) due to its security significance. Each person who produces, receives, or acquires SGI shall ensure that it is protected against unauthorized disclosure. To meet this requirement, organizations and persons shall establish, implement, and maintain a system to protect SGI consistent with the requirements set forth in 10 CFR 73.21.

Persons Subject to These Requirements

Any person who produces, receives, or acquires SGI—regardless of whether he or she is a member of an entity or organization that the NRC regulates—is subject to the requirements (and sanctions) of 10 CFR 73.21. An organization or person that possesses SGI must inform contractors and suppliers that handle SGI of the existence of regulatory requirements and the need for proper protection (see additional guidance prescribed by 10 CFR 73.22 and referenced within this guidance document below). Federal, State, Tribal, or local law enforcement agencies with access to SGI also are subject to the regulatory requirements of 10 CFR 73.21. However, the NRC presumes that these law enforcement agencies have adequate information protection systems. The requirements under which entities may transfer information to a third party (i.e., on a need-to-know basis), still apply to law enforcement agencies, as do sanctions for unlawful disclosure. Entities or organizations that have arrangements with law enforcement agencies should advise them of the existence of the information protection requirements under 10 CFR 73.22 "Protection of Safeguards Information: Specific Requirements."

Criminal and Civil Sanctions

The Atomic Energy Act of 1954, as amended, (AEA, the Act), Section 147a, explicitly provides that any person, "whether or not a licensee of the Commission, who violates any regulations adopted under this section shall be subject to the civil monetary penalties of section 234 of this Act." Furthermore, willful violation of any regulation or Order governing SGI is a felony subject to criminal penalties in the form of fines or imprisonment, or both. (See Sections 147b and 223 of the Act.)

Information to be Protected

The types of information and documents that must be protected as SGI are described in 10 CFR 73.22(a) and include, but are not limited to, nonpublic, security-related requirements such as the following:

(1) *Physical protection.* This requirement includes non-public security related information not classified as Restricted Data or National Security Information about physical protection of source, byproduct, or special nuclear material.

(2) *Physical protection in transit*. This requirement includes information about the transportation of, or delivery to a carrier for transportation of, irradiated reactor fuel, including the following:

(i) 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 SGI 10 days after the last shipment of a current series.

(ii) Arrangements with and specific capabilities of local police response forces (information that isn't already publicly available) and locations of safe havens identified along the transportation route.

Conditions for Access

Consistent with the requirements set forth in 10 CFR 73.22(b), to gain access to SGI for its employees, agents, or contractors, an entity or organization must have an appropriate need-to-know determination from the possessor of the SGI, a Federal Bureau of Investigation (FBI) fingerprint criminal-history records check, and be deemed trustworthiness and reliability based on a background check. The Tribal official, Tribal official's designated representative, and Tribal law enforcement personnel are relieved from the requirement for an FBI fingerprint criminal-history records check and other elements of the background check prior to being granted access to SGI information. The NRC has determined that Tribal officials, Tribal official's designated representatives, and Tribal law enforcement personnel who are designated to receive advance notifications for shipments of irradiated reactor fuel and certain nuclear wastes that may be transported within or across Tribal reservations have established a need to know for access to SGI.

Protection While in Use

Consistent with the requirements set forth in 10 CFR 73.22(c), while in use, SGI shall be under the control of an authorized individual who meets the requirements for access to SGI. The primary consideration is limiting SGI access to those who have authorized access and an established need-to-know for the information. For Tribes, this individual is the person that has met the SGI access requirements and is designated by the Tribal official to receive the advance notifications for shipments of irradiated reactor fuel and certain nuclear wastes that may be transported within or across Tribal reservations.

Protection While in Storage

Consistent with the requirements set forth in 10 CFR 73.22(c), while unattended, SGI shall be stored in an approved security storage container, meaning (1) a steel filing cabinet (located within a controlled access facility) equipped with a steel locking bar and a three-position, changeable combination GSA approved padlock, or (2) a security filing cabinet marked "General

Services Administration Approved Security Container" on the exterior of the top drawer or door. Entities shall limit knowledge of lock combinations or access to keys protecting SGI to a minimum number of personnel who have a need-to-know for operating purposes and are otherwise authorized access to SGI in accordance with regulatory requirements. Entities shall strictly control access to lock combinations or keys to prevent their disclosure or release to an unauthorized individual.

Reproduction of Matter Containing SGI

Consistent with the requirements set forth in 10 CFR 73.22(e), possessors of SGI may reproduce it to the minimum extent necessary without permission of the originator. Digital copiers that scan and retain images of documents represent a potential security concern. Entities and organizations must evaluate copiers used to reproduce SGI to ensure that unauthorized personnel cannot obtain SGI through memory retention or network connectivity. Organizations should clearly identify copiers used to reproduce SGI as being approved for the reproduction of SGI and place them in a location that discourages surreptitious use and ensures control over the machine's immediate proximity.

Transportation of Documents and Other Matter

Consistent with the requirements set forth in 10 CFR 73.22(f), when transporting documents containing SGI outside an authorized place of use or storage, possessors of the information shall enclose it in two sealed envelopes or wrappers. The inner envelope or wrapper shall 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, contain the address of the intended recipient and the address of the sender, and must not bear any markings or indication that the envelope or wrapper contains SGI. Any commercial delivery company that offers computerized tracking features may transport SGI (U.S. First Class, Registered, Express, or Certified Mail). Any individual authorized access under regulatory requirements may also transport SGI. Within a facility, individuals may transport SGI in a single opaque envelope or wrapper—or without single or double wrapping—provided that employees take adequate measures to protect the material against unauthorized disclosure. Individuals who transport SGI should keep the documents in their personal possession at all times or ensure that the information is appropriately secured to prevent unauthorized disclosure.

Processing of SGI on Electronic Systems

Consistent with the requirements set forth in 10 CFR 73.22(g), entities and organizations may transmit SGI over an open network, provided that the e-mail system encrypts messages on a standalone computer or computer system using a method that the NRC has approved. In such instances, the organization will select a commercially available encryption system that the National Institute of Standards and Technology (NIST) has validated as conforming to Federal Information Processing Standard (FIPS) 140-2, "Security Requirements for Cryptographic Modules," or later. Request for the approval of a selected encryption system must be forwarded to the NRC prior to use for encrypting and transmitting SGI.

The NRC only approves encryption methods for SGI that meet FIPS 140-2 or later. NIST maintains a listing of all validated encryption systems at http://csrc.nist.gov/cryptval/140-1/1401val.htm.

Telecommunications

Consistent with the requirements set forth in 10 CFR 73.22(f), organizations may not transmit SGI over unprotected telecommunications circuits except under emergency or extraordinary conditions. Only an NRC-approved secure electronic device, such as a secure facsimile or secure telephone device, shall transmit SGI outside an authorized place of use or storage, provided that the transmitter and receivers implement procedures that will ensure that SGI is protected before and after the transmission or e-mail. For the purpose of this requirement, "emergency or extraordinary conditions" are defined as any circumstances that require immediate communications to report, summon assistance for, or respond to a security event (or an event that has potential security significance).

Destruction

Consistent with the requirements set forth in 10 CFR 73.22(i), possessors of documents containing SGI shall destroy them when they are no longer needed. Burning and shredding are acceptable methods of destruction that prevent members of the public at large from reconstructing documents by means available to them. A document is considered completely destroyed when it is in pieces measuring one-quarter inch or smaller and mixed with several pages or documents. The pieces, when measured, must not be wider than one-quarter inch vertically or horizontally.

Additional information on the protection of SGI is available in Regulatory Guide 5.79, "PROTECTION OF SAFEGUARDS INFORMATION," which is available on the NRC website at http://pbadupws.nrc.gov/docs/ML1032/ML103270219.pdf.