

March 6, 2007

The Honorable Eliot Spitzer
Governor of New York
Albany, New York 12224

Dear Governor Spitzer:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am writing to request that you appoint a State Liaison Officer to act as the primary liaison to the NRC. I am also writing to provide an explanation of our process for the distribution of NRC security information to State contacts and of the requirements for protecting this information.

Former Governor Pataki previously had appointed Peter Smith, President, New York State Energy Research and Development Authority, as the State Liaison Officer for New York. Unless you designate a new State Liaison Officer, we will continue to keep you informed of our programs and activities through Mr. Smith. At the same time, we also will continue to work with other individuals in State agencies with whom we have established relationships.

In 1976, the NRC adopted a recommendation from several State organizations, including the National Governors Association, that we request each State to appoint a single person to act as a liaison to the NRC for the purpose of improving Federal/State cooperation. The NRC relies on the Governor-appointed State Liaison Officer to provide the primary communication channel between the States and the NRC. The State Liaison Officer serves as the key person in the State to keep the Governor informed on issues under the NRC's jurisdiction (specifically matters addressing nuclear regulation, nuclear security, and radiological public health and safety), and provides NRC with State information on particular nuclear safety, security, or environmental issues.

As a result of the September 11, 2001, terrorist attacks, the NRC has increased its communications with the Governor-appointed State Liaison Officers. State Liaison Officers' responsibilities have changed and are continuing to evolve. Moreover, there is an increased need to ensure that other State officials with a "need-to-know" have access to information that may be classified or sensitive unclassified, which includes Safeguards Information (SGI). SGI is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act of 1954, as amended, to be protected from inadvertent release and unauthorized disclosure. SGI is handled and protected more like classified National Security Information than like other sensitive unclassified information. Sensitive unclassified information includes Official Use Only and Proprietary Information in addition to SGI, is not available to the public, and requires extra measures of protection.

Your appointed State Liaison Officer should continue to serve as the primary recipient for sensitive unclassified information, including SGI, from NRC. However, because of the State Homeland Security Advisors' responsibility for homeland security activities in the States, these State officials will also be provided copies of NRC security information in coordination with the Department of Homeland Security. This will help ensure that the State Homeland Security Advisor has knowledge of and access to this information and can also share such information with other authorized State officials on a need-to-know basis.

State Liaison Officers, and other State officials having access to sensitive unclassified information, also need to exercise the appropriate precautions to protect the information from unauthorized disclosure. Regulatory Issue Summary (RIS) 2003-08, Protection of Safeguards Information from Unauthorized Disclosure, is contained in Enclosure 1. Enclosure 2 contains additional detailed information about SGI handling and protection requirements, including: (1) sharing SGI with those who, by reason of position, have a need-to-know; (2) protection while in use or storage; (3) preparation and marking; (4) external transmission; (5) reproduction and destruction; and (6) criminal and civil sanctions.

If you or your staff have any questions concerning this correspondence or wish to obtain additional information about the State Liaison Officer program, please contact Dennis K. Rathbun, Director, Division of Intergovernmental Liaison and Rulemaking, Office of Federal and State Materials and Environmental Management Programs, in Headquarters at 301-415-2325, or by e-mail at dkr@nrc.gov.

I thank you in advance for your assistance and look forward to continuing an excellent working relationship with the State of New York.

Sincerely,

/RA/

Dale E. Klein

Enclosures:

1. RIS 2003-08, *Protection of Safeguards Information from Unauthorized Disclosure*
2. Safeguards Information Protection Requirements

cc: Peter Smith
State Liaison Officer

Safeguards Information Protection Requirements

Authority

The Atomic Energy Act of 1954, as amended, 42 U.S.C. §§ 2011 *et seq.* (Act), grants the U.S. Nuclear Regulatory Commission (NRC) broad and unique authority to prohibit the unauthorized disclosure of Safeguards Information upon a determination that the unauthorized disclosure of such 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 materials or facilities subject to NRC jurisdiction. Section 147 of the Act, 42 U.S.C. § 2167.

In addition to the licensees subject to the Safeguards Information requirements of 10 CFR Part 73, and the types of information designated as Safeguards Information under those regulations, the Commission has authority under Section 147 to designate, by regulation or Order, other types of information as Safeguards Information. This authority extends to information concerning special nuclear material, source material, and byproduct material, as well as production and utilization facilities. The Commission also may, by Order, impose Safeguards Information handling requirements on these other licensees. All licensees and all other persons who now have, or in the future may have, access to Safeguards Information must comply with all applicable requirements delineated in regulations and Orders governing the handling and unauthorized disclosure of Safeguards Information.

Definition of Safeguards Information for Licensees and Any Other Persons Subject to Part 73 Requirements

Safeguards Information is defined by NRC regulation [Section 73.2 of Title 10 of the *Code of Federal Regulations* (10 CFR 73.2)] as follows:

Safeguards Information means information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

In addition to the licensees subject to the Safeguards Information requirements of Part 73, and the types of information designated as Safeguards Information under those regulations, the Commission has authority under Section 147 of the AEA to designate, by regulation or Order, other types of information as Safeguards Information. For example, Section 147 allows the Commission to designate as Safeguards Information a licensee's or applicant's detailed:

- (1) Control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or common defense and security;

- (2) Security measures (including security plans, procedures and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; or
- (3) Security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials covered by paragraphs (1) and (2) if the unauthorized disclosure of such 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 such material or such facility.

Generally, definitions (1), (2), and (3) above are referred to by the acronym “SGI;” however, SGI for byproduct or source material subject to modified (from 10 CFR Part 73) handling requirements is also referred to as “Safeguards Information - Modified Handling” or SGI-M to distinguish its handling requirements and associated consequence levels. Information represented by both acronyms are considered Safeguards Information.

General Performance Requirement

Any person who produces, receives, or acquires SGI shall ensure that it is protected against unauthorized disclosure. To meet this requirement, licensees and persons shall establish and maintain an information protection system that includes the specific measures listed below. Information protection procedures employed by State and local police forces are deemed to meet these requirements.

Persons Subject to These Requirements

Any person, whether or not a licensee of the NRC, who produces, receives, or acquires SGI is subject to the requirements and sanctions as authorized by Section 147 of the Atomic Energy Act of 1954, as amended, and are more fully described in 10 CFR 73.21 or by the NRC in the form of Orders. A State and its employees would fall under this requirement if they possess SGI. Individuals authorized access to SGI by the State and its employees should be informed as to the existence of regulatory requirements and the need for proper protection. (See additional information under Conditions for Access.)

State or local police units who have access to SGI also are subject to this requirement. However, these organizations are deemed in the requirements of 10 CFR 73.21 and relevant Orders to have adequate information protection systems. The conditions for transfer of information to a third party, i.e., need-to-know, would still apply to the police organization as would sanctions for unlawful disclosure.

Criminal and Civil Sanctions (Sections 223 and 234 of the Atomic Energy Act)

The Act 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.” Section 147a of the Act. Furthermore, willful violation of any regulation or Order governing safeguards information is a felony subject to criminal penalties in the form of fines or imprisonment, or both. See Sections 147b and 223 of the Act.

Categories of Safeguards Information and Protection Levels

SGI is divided into two categories of protected information. Information defined by 10 CFR 73.21(a) applies primarily to special nuclear material (e.g., commercial nuclear reactor or transportation of irradiated fuel) and is designated as SGI. For byproduct material licensees under NRC regulation, the NRC issued Orders requiring specific security measures. This information was designated as Safeguards Information-Modified Handling (SGI-M). This information has been designated as SGI-M because unauthorized disclosure 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 materials. The designation of information as SGI-M refers to the marking used to denote modified protection requirements; however, the information is still SGI.

Differences in protection levels for SGI and SGI-M due to potential consequences of compromise are addressed below:

Conditions for Access

While there are no personnel security clearances required for access to SGI, a determination of trustworthiness and need-to-know are required for access to this information. The conditions for access are set forth below.

Need-to-Know

Need-to-know is defined as a determination by a person having responsibility for protecting SGI that a proposed recipient's access to SGI is necessary in the performance of official, contractual, or licensee duties of employment. A person in possession of SGI has discretionary authority in making these determinations. The recipient should be made aware that the information is sensitive, subject to NRC regulations and Orders as well as criminal and civil sanctions.

Occupational Groups

In lieu of a personnel security clearance program (such as that required by Government classified programs), dissemination of SGI is limited to members of certain occupational groups who have a need-to-know such information. These include:

- (1) An employee, agent, or contractor of an applicant, a licensee, the Commission, or the United States Government;
- (2) A member of a duly authorized committee of the Congress;
- (3) The Governor of a State or his designated representative;
- (4) A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC;
- (5) A member of a State or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies; or
- (6) A person to whom disclosure is ordered pursuant to Section 2.744 of Part 2 of Title 10 of the Code of Federal Regulations.

NRC Orders relating to security measures for byproduct materials licensees have added a seventh occupational group to the list of individuals who can access SGI-M information:

- (7) State Radiation Control Program Directors (and State Homeland Security Directors) or their designees.

Generally, individuals are considered to be trustworthy by virtue of their employment status; however, background checks, for some of the above groups, are required to be performed by the employer in addition to verification of employment status. Nevertheless, some discretion should be exercised in granting access if there is any indication that the recipient would be unwilling or unable to provide proper protection for the SGI.

Protection While in Use or Storage

While in use, matter containing SGI shall be under the control of an authorized individual. This requirement is satisfied if the matter is attended by an authorized individual even though the information is in fact not constantly being used.

While unattended, SGI shall be stored in a locked security storage container as described in 10 CFR 73.2. Information containing SGI-M shall be stored in a locked file drawer or container. Knowledge of lock combinations or access to keys, where applicable, protecting SGI shall be limited to a minimum number of personnel for operating purposes who have a "need-to-know" and are otherwise authorized access to SGI in accordance with the provisions of the regulations or an NRC Order. Access to lock combinations or keys shall be strictly controlled so as to prevent disclosure to an unauthorized individual.

Transmission/Transportation of Documents and Other Matter

Documents containing SGI when transmitted outside an authorized place of use or storage shall be enclosed in two sealed envelopes or wrappers to preclude disclosure of the presence of protected information. The inner envelope or wrapper shall contain the name and address of the intended recipient, and be marked, on top and bottom on both sides, with the words "**Safeguards Information**" or "**Safeguards Information-Modified Handling**" as appropriate. The outer envelope or wrapper must be addressed to the intended recipient, must contain the address of the sender, and must not bear any markings or indication that the document contains Safeguards Information.

SGI may be transported by messenger-courier, U.S. first class, registered, express, or certified mail, or by any individual authorized access pursuant to the regulations or an NRC Order. Individuals transporting SGI should retain the documents or other matter in their personal possession at all times or ensure that it is appropriately wrapped and also secured to preclude compromise by an unauthorized individual.

Except under emergency or extraordinary conditions, SGI shall be transmitted only by protected telecommunications circuits (including facsimile) approved by the NRC.

Marking of Documents

Each document that contains SGI should have on the face of the document (i) the name, title, and organization of the individual authorized to make a SGI determination, and who has determined that the document contains SGI, (ii) the date the document was originated or the

determination made, (iii) an indication that the document contains SGI, and (iv) an indication that unauthorized disclosure would be subject to civil and criminal sanctions. Each page shall be marked in a conspicuous fashion denoting “**Safeguards Information**” or “**Safeguards Information-Modified Handling**.”

Transmittal letters or memoranda which do not in themselves contain SGI should be marked to indicate that attachments or enclosures contain SGI.

In addition to the information required on the face of the document, each item of correspondence that contains SGI, should by marking or other means clearly indicate which portions (e.g., paragraphs, pages, or appendices) contain SGI and which do not. (Portion marking is not required for the specific items of information set forth in 10 CFR 73.21(b) other than guard qualification and training plans and correspondence to and from the NRC).

All documents or other matter in use or storage should be marked in accordance with the regulations or NRC Orders. A specific exception is provided for documents in the possession of contractors and agents of licensees that were produced more than one year prior to the effective date of the regulations or NRC Orders. Such documents need to be marked once they are removed from file drawers, containers, or security storage containers. The same exception would also apply to old documents stored away from the facility in central files or corporation headquarters.

Since information protection procedures employed by State and local police forces are deemed to meet NRC requirements, documents in the possession of these agencies need not be marked as set forth in this document.

Reproduction of Matter Containing SGI

SGI may be reproduced to the minimum extent necessary consistent with need without permission of the originator.

Use of Automatic Data Processing (ADP) Systems

SGI may be processed or produced on an ADP system provided that the system is self-contained within the SGI holder's facility and requires the use of an entry code for access to stored information. An ADP system is defined here as a data processing system having the capability of long term storage of SGI. Word processors such as typewriters are not subject to the requirements as long as they do not transmit information off-site. The objective of these restrictions is to prevent access and retrieval of stored SGI by unauthorized individuals, particularly from remote terminals. Specific files containing SGI will be password protected to preclude access by an unauthorized individual. Files may be transmitted over a network if the file is encrypted. The National Institute of Standards and Technology (NIST) maintains a listing of all validated encryption systems at <http://csrc.nist.gov/cryptval/140-1/1401val.htm>. SGI files shall be properly labeled as “**Safeguards Information**” or “**Safeguards Information-Modified Handling**,” as appropriate, and saved to removable media and stored in an appropriately locked container. A security storage container as defined in 10 CFR 73.2 is appropriate for SGI information. A locked file drawer or cabinet is appropriate for SGI-M information as required by NRC Order.

Removal From SGI Category

Documents originally containing SGI shall be removed from the SGI category whenever the information no longer meets the criteria contained in this Section.

Documents should only be removed from the SGI category by, or with the permission of, the individual (or office) who made the original determination. The document should indicate the name and organization of the individual removing the document from the SGI category and the date of the removal. Other persons who have the document in their possession should be notified of the removal.

Telecommunications

SGI may not be transmitted by unprotected telecommunications circuits except under emergency or extraordinary conditions. For the purpose of this requirement, 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 event (or an event that has potential security significance).

This restriction applies to telephone, telegraph, teletype, facsimile circuits, and to radio. Routine telephone or radio transmission between site security personnel, or between the site and local police, should be limited to message formats or codes that do not disclose facility security features or response procedures. Similarly, call-ins during transport should not disclose the point of transmission or schedule information. (Infrequent or non-repetitive telephone conversations regarding a physical security plan or program are permitted provided that either the discussion is general in nature or the identification of specific safeguards measures is effectively disguised.)

Individuals should use care when discussing SGI at meetings or in the presence of others to insure that the conversation is not overheard by persons not authorized access. Transcripts or minutes of meetings or hearings that contain SGI should be marked and protected in accordance with the regulations or NRC Order.

Destruction

Documents containing SGI may be destroyed by tearing into small pieces, burning, shredding or any other method that precludes reconstruction by means available to the public at large. Piece sizes one half inch or smaller composed of several pages or documents and thoroughly mixed would be considered completely destroyed.