

UNITED STATES
NUCLEAR REGULATORY COMMISSION

In the Matter of

EA-06-193

LOUISIANA ENERGY SERVICES, L.P.

(National Enrichment Facility)

AND ALL OTHER PERSONS WHO SEEK

OR OBTAIN ACCESS TO SAFEGUARDS

INFORMATION DESCRIBED HEREIN

**ORDER IMPOSING REQUIREMENTS FOR THE
PROTECTION OF SAFEGUARDS INFORMATION
AND ACCESS TO NEW SAFEGUARDS INFORMATION
(EFFECTIVE IMMEDIATELY)**

I

Louisiana Energy Services, L.P., (LES or the Licensee) holds a license, issued in accordance with the Atomic Energy Act (AEA) of 1954, by the U.S. Nuclear Regulatory Commission (NRC or Commission) authorizing it to construct and operate a uranium

enrichment facility in Lea County, New Mexico. On March 19, 2004, in accordance with Commission direction in Staff Requirements Memorandum SECY-03-0083, NRC provided LES, for its information, copies of Orders issued to Category III facilities on interim measures to enhance physical security at those facilities. Those Orders contained Safeguards Information¹. In addition, in the future, the Commission may issue the Licensee additional Orders that require compliance with specific Additional Security Measures to enhance the security. These Orders are also expected to contain Safeguards Information, which cannot be released to the public and must be protected from unauthorized disclosure. Therefore, the Commission is imposing the requirements, as set forth in Attachments A and B of this Order, so that the Licensee can receive these documents. This Order also imposes requirements for the protection of Safeguards Information in the hands of any person,² whether or not a licensee of the Commission, who produces, receives, or acquires Safeguards Information.

On August 8, 2005, the Energy Policy Act of 2005 (EPAAct) was enacted. Section 652 of the EPAAct amended Section 149 of the AEA to require fingerprinting and a Federal Bureau of Investigation (FBI) identification and criminal history records check of any person who is to be permitted to have access to Safeguards Information. The NRC's implementation of this requirement cannot await the completion of the Safeguards Information rulemaking, which is

¹Safeguards Information is a form of sensitive, unclassified, security-related information that the Commission has the authority to designate and protect under section 147 of the AEA.

² 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, except that the Department of Energy shall be considered a person with respect to those facilities of the Department specified in section 202 of the Energy Reorganization Act of 1974 (88 Stat. 1244), any State or any political subdivision of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent, or agency of the foregoing.

underway, because the EAct fingerprinting and criminal history check requirements for access to Safeguards Information were immediately effective upon enactment of the EAct. Although the EAct permits the Commission by rule to except certain categories of individuals from the fingerprinting requirement, which the Commission has done (see 10 CFR § 73.59, 71 Fed. Reg. 33,989 (June 13, 2006)), it is unlikely that many Licensee employees are excepted from the fingerprinting requirement by the “fingerprinting relief” rule. Individuals relieved from the fingerprinting and criminal history checks under the relief rule include Federal, State, and local officials and law enforcement personnel; Agreement State inspectors, who conduct security inspections on behalf of the NRC; members of Congress and certain employees of members of Congress or Congressional Committees; representatives of the International Atomic Energy Agency or certain foreign government organizations. In addition, individuals who have active Federal security clearances and have satisfied the EAct fingerprinting requirement need not be fingerprinted again. Therefore, in accordance with Section 149 of the AEA, as amended by the EAct, the Commission is imposing additional requirements, as set forth by this Order, for access to new Safeguards Information³ by any person, from any person, whether or not a Licensee, Applicant, or Certificate Holder of the Commission or Agreement States.

II

The Commission has broad statutory authority to protect Safeguards Information and prohibit its unauthorized disclosure. Section 147 of the AEA, as amended, grants the Commission explicit authority to “... issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information” Furthermore, Section 652 of the

³ “New Safeguards Information” means Safeguards Information generated subsequent to August 8, 2005, the date of enactment of the EAct. “New Safeguards Information” also means any Safeguards Information, regardless of when it was generated, that is being accessed by an individual who has never been previously granted access to Safeguards Information.

EPA Act amended Section 149 of the AEA to require fingerprinting and an FBI identification and a criminal history records check of each individual who seeks access to Safeguards Information. Licensees and all persons who produce, receive, or acquire Safeguards Information must ensure proper handling and protection of Safeguards Information, to avoid unauthorized disclosure, in accordance with the specific requirements for the protection of Safeguards Information contained in Attachments A and B. The Commission hereby provides notice that it intends to treat violations of the requirements contained in Attachments A and B, applicable to the handling and unauthorized disclosure of Safeguards Information, as serious breaches of adequate protection of the public health and safety and the common defense and security of the United States. Access to Safeguards Information is limited to those persons who have established a need-to-know the information, and are considered to be trustworthy and reliable, and who satisfy the fingerprinting and criminal history records check required by the EPA Act and this Order. A “need-to-know” means a determination by a person having responsibility for protecting Safeguards Information that a proposed recipient's access to Safeguards Information is necessary in the performance of official, contractual, or licensee duties of employment. The Licensee and all other persons who obtain Safeguards Information must ensure that they develop, maintain, and implement strict policies and procedures for the proper handling of Safeguards Information, to prevent unauthorized disclosure, in accordance with the requirements in Attachments A and B. The Licensee must ensure that all contractors whose employees may have access to Safeguards Information either adhere to the Licensee’s policies and procedures on Safeguards Information or develop, maintain, and implement their own acceptable policies and procedures. The Licensee remains responsible for the conduct of its contractors. The policies and procedures necessary to ensure compliance with applicable requirements contained in Attachments A and B must address, at a minimum, the following: (1) the general performance requirement that each person who produces, receives, or acquires

Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure; (2) protection of Safeguards Information at fixed sites, in use and in storage, and while in transit; (3) correspondence containing Safeguards Information; (4) access to Safeguards Information; (5) preparation, marking, reproduction, and destruction of documents; (6) external transmission of documents; (7) use of automatic data processing systems; and (8) removal of the Safeguards Information category.

To provide assurance that the Licensee is implementing appropriate measures to achieve a consistent level of protection to prohibit the unauthorized disclosure of new Safeguards Information, the Licensee shall implement the fingerprinting and criminal history check requirements for access to new Safeguards Information in this Order, as well as the requirements in Attachments A and B of this Order. In addition, pursuant to 10 CFR § 2.202, I find that in light of the common defense and security matters identified above, which warrant the issuance of this Order, the public health, safety, and interest require that this Order be effective immediately.

III

Accordingly, pursuant to Sections 53, 62, 63, 81, 147, 149, 161b, 161i, 161o, 182, and 186 of the Atomic Energy Act of 1954, as amended, and the Commission's regulations in 10 CFR § 2.202, 10 CFR Part 30, 10 CFR Part 40, and 10 CFR Part 70, IT IS HEREBY ORDERED, **EFFECTIVE IMMEDIATELY**, THAT LICENSEE AND ALL OTHER PERSONS WHO PRODUCE, RECEIVE, OR ACQUIRE THE ADDITIONAL SECURITY MEASURES IDENTIFIED ABOVE (WHETHER DRAFT OR FINAL), OR WHO SEEK OR OBTAIN ACCESS TO NEW SAFEGUARDS INFORMATION, SHALL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS ORDER, INCLUDING THE REQUIREMENTS IN ATTACHMENTS A AND B.

- A. No person may have access to new Safeguards Information unless that person has a need-to-know the new Safeguards Information, has been fingerprinted and undergone an FBI identification and criminal history records check, which has been favorably decided, and satisfies all other applicable requirements for access to Safeguards Information. Fingerprinting and the FBI identification and criminal history records check are not required, however, for any person who is relieved from that requirement by 10 CFR § 73.59 (71 Fed. Reg. 33,989 (June 13, 2006)) or who has an active Federal security clearance.
- B. No person may provide new Safeguards Information to any other person except in accordance with condition III.A above. Prior to sharing new Safeguards Information with any other person, a copy of this Order shall be provided to that person.

IV.

The Director, Office of Nuclear Material Safety and Safeguards, may, in writing, relax or rescind any of the above conditions, on demonstration of good cause by the Licensee. In accordance with 10 CFR § 2.202, the Licensee must, and any other person adversely affected by this Order may, submit an answer to this Order, and may request a hearing on this Order, within twenty (20) days of the date of this Order. Where good cause is shown, consideration will be given to extending the time to request a hearing. A request for extension of time in which to submit an answer or request a hearing must be made in writing to the Director, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555, and include a statement of good cause for the extension. The answer may consent to this Order. Unless the answer consents to this Order, the answer shall, in writing and under oath or affirmation, specifically set forth the matters of fact and law on which the Licensee or other person adversely affected relies, and the reasons as to why the Order should not have

been issued. Any answer or request for a hearing shall be submitted to the Secretary, Office of the Secretary, U.S. Nuclear Regulatory Commission, ATTN: Rulemakings and Adjudications Staff, Washington, DC 20555. Copies also shall be sent to the Director, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC 20555; to the Assistant General Counsel for Materials Litigation and Enforcement, at the same address; and to the Licensee, if the answer or hearing request is by a person other than the Licensee. Because of possible delays in delivery of mail to United States Government offices, it is requested that answers and requests for hearing be transmitted to the Secretary of the Commission, either by means of facsimile transmission, to 301-415-1101, or by e-mail, to hearingdocket@nrc.gov; and also to the Office of the General Counsel, either by means of facsimile transmission, to 301-415-3725, or by e-mail, to OGCMailCenter@nrc.gov. If a person other than the Licensee requests a hearing, that person shall set forth with particularity the manner in which their interest is adversely affected by this Order and shall address the criteria set forth in 10 CFR § 2.309.

If a hearing is requested by the Licensee or a person whose interest is adversely affected, the Commission will issue an Order designating the time and place of any hearing. If a hearing is held, the issue to be considered at such hearing shall be whether this Order should be sustained.

Pursuant to 10 CFR § 2.202(c)(2)(i), the Licensee may, in addition to demanding a hearing, at the time the answer is filed or sooner, move the presiding officer to set aside the immediate effectiveness of the Order on the grounds that the Order, including the need for immediate effectiveness, is not based on adequate evidence, but on mere suspicion, unfounded allegations, or error. In the absence of any request for hearing, or written approval

of an extension of time in which to request a hearing, the provisions specified in Section III above shall be final twenty (20) days from the date of this Order, without further order or proceedings. If an extension of time for requesting a hearing has been approved, the provisions specified in Section III shall be final when the extension expires, if a hearing request has not been received.

AN ANSWER OR A REQUEST FOR HEARING SHALL NOT STAY THE IMMEDIATE
EFFECTIVENESS OF THIS ORDER.

Dated at Rockville, Maryland this 28th day of August 2006

For the Nuclear Regulatory Commission

/RA/

Jack R. Strosnider, Director
Office of Nuclear Material Safety
and Safeguards

Attachment A

Modified Handling Requirements for the Protection of Certain Safeguards Information (SGI-M)

General Requirement

Information and material that the U.S. Nuclear Regulatory Commission (NRC) determines are safeguards information must be protected from unauthorized disclosure. In order to distinguish information needing modified protection requirements from the safeguards information for reactors and fuel cycle facilities that require a higher level of protection, the term "Safeguards Information-Modified Handling" (SGI-M) is being used as the distinguishing marking for certain materials licensees. Each person who produces, receives, or acquires SGI-M 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 measures specified 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-M is subject to the requirements (and sanctions) of this document. Firms and their employees that supply services or equipment to materials licensees fall under this requirement if they

possess SGI-M. A licensee must inform contractors and suppliers of the existence of these requirements and the need for proper protection. (See more under Conditions for Access)

State or local police units who have access to SGI-M are also subject to these requirements. However, these organizations are deemed 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. Again, it would be prudent for licensees who have arrangements with local police to advise them of the existence of SGI-M requirements.

Criminal and Civil Sanctions

The Atomic Energy Act of 1954, as amended, 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 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.*

Conditions for Access

Access to SGI-M beyond the initial recipients of the order will be governed by the background check requirements imposed by the order. Access to SGI-M by licensee employees, agents, or contractors must include both an appropriate need-to-know determination by the licensee, as well as a determination concerning the trustworthiness of individuals having access to the information. Employees of an organization affiliated with the licensee's company, e.g., a parent company, may be considered as employees of the licensee for access purposes.

Need-to-Know

Need-to-know is defined as a determination by a person having responsibility for protecting SGI-M that a proposed recipient's access to SGI-M is necessary in the performance of official, contractual, or licensee duties of employment. The recipient must be made aware that the information is SGI-M and those having access to it are subject to these requirements as well as criminal and civil sanctions for mishandling the information.

Occupational Groups

Dissemination of SGI-M is limited to individuals who have an established need-to-know and who are members of certain occupational groups. These occupational groups are:

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;
6. A person to whom disclosure is ordered pursuant to Section 2.744(e) of Part 2 of part 10 of the Code of Federal Regulations; or
7. State Radiation Control Program Directors (and State Homeland Security Directors) or their designees.

In a generic sense, the individuals described above in (A) through (G) are considered to be trustworthy by virtue of their employment status. For non-governmental individuals in group (A) above, a determination of reliability and trustworthiness is required. Discretion must be exercised in granting access to the individuals in group (A). If there is any indication that the recipient would be unwilling or unable to provide proper protection for the SGI-M, they are not authorized to receive SGI-M.

Information Considered for Safeguards Information Designation

Information deemed SGI-M is information the disclosure of which 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.

SGI-M identifies safeguards information which is subject to these requirements. These requirements are necessary in order to protect quantities of nuclear material significant to the health and safety of the public or common defense and security.

The overall measure for consideration of SGI-M is the usefulness of the information (security or otherwise) to an adversary in planning or attempting a malevolent act. The specificity of the information increases the likelihood that it will be useful to an adversary.

Protection While in Use

While in use, SGI-M shall be under the control of an authorized individual. This requirement is satisfied if the SGI-M is attended by an authorized individual even though the information is in fact not constantly being used. SGI-M, therefore, within alarm stations, continuously manned guard posts or ready rooms need not be locked in file drawers or storage containers.

Under certain conditions the general control exercised over security zones or areas would be considered to meet this requirement. The primary consideration is limiting access to those who have a need-to-know. Some examples would be:

Alarm stations, guard posts and guard ready rooms;

Engineering or drafting areas if visitors are escorted and information is not clearly visible;

Plant maintenance areas if access is restricted and information is not clearly visible;

Administrative offices (e.g., central records or purchasing) if visitors are escorted and information is not clearly visible;

Protection While in Storage

While unattended, SGI-M shall be stored in a locked file drawer or container. Knowledge of lock combinations or access to keys protecting SGI-M 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-M in accordance with these requirements. Access to lock combinations or keys shall be strictly controlled so as to prevent disclosure to an unauthorized individual.

Transportation of Documents and Other Matter

Documents containing SGI-M when transmitted outside an authorized place of use or storage shall be enclosed in two sealed envelopes or wrappers. The inner envelope or wrapper shall contain the name and address of the intended recipient, and be marked both sides, top and bottom with the words “**Safeguards Information - Modified Handling.**” 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 SGI-M.

SGI-M may be transported by any commercial delivery company that provides nation-wide overnight service with computer tracking features, US first class, registered, express, or certified mail, or by any individual authorized access pursuant to these requirements.

Within a facility, SGI-M may be transmitted using a single opaque envelope. It may also be transmitted within a facility without single or double wrapping, provided adequate measures are taken to protect the material against unauthorized disclosure. Individuals transporting SGI-M should retain the documents in their personal possession at all times or ensure that the information is appropriately wrapped and also secured to preclude compromise by an unauthorized individual.

Preparation and Marking of Documents

While the NRC is the sole authority for determining what specific information may be designated as “SGI-M,” originators of documents are responsible for determining whether those

documents contain such information. Each document or other matter that contains SGI-M shall be marked "**Safeguards Information - Modified Handling**" in a conspicuous manner on the top and bottom of the first page to indicate the presence of protected information. The first page of the document must also contain (i) the name, title, and organization of the individual authorized to make a SGI-M determination, and who has determined that the document contains SGI-M, (ii) the date the document was originated or the determination made, (iii) an indication that the document contains SGI-M, and (iv) an indication that unauthorized disclosure would be subject to civil and criminal sanctions. Each additional page shall be marked in a conspicuous fashion at the top and bottom with letters denoting "**Safeguards Information - Modified Handling.**"

In addition to the "**Safeguards Information - Modified Handling**" markings at the top and bottom of page, transmittal letters or memoranda which do not in themselves contain SGI-M shall be marked to indicate that attachments or enclosures contain SGI-M but that the transmittal does not (e.g., "When separated from SGI-M enclosure(s), this document is decontrolled").

In addition to the information required on the face of the document, each item of correspondence that contains SGI-M shall, by marking or other means, clearly indicate which portions (e.g., paragraphs, pages, or appendices) contain SGI-M and which do not. Portion marking is not required for physical security and safeguards contingency plans.

All documents or other matter containing SGI-M in use or storage shall be marked in accordance with these requirements. 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 order. Such documents need not be marked unless they are removed from file drawers or containers. The same exception applies 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.

Removal from SGI-M Category

Documents containing SGI-M shall be removed from the SGI-M category (decontrolled) only after the NRC determines that the information no longer meets the criteria of SGI-M. Licensees have the authority to make determinations that specific documents which they created no longer contain SGI-M information and may be decontrolled. Consideration must be exercised to ensure that any document decontrolled shall not disclose SGI-M in some other form or be combined with other unprotected information to disclose SGI-M.

The authority to determine that a document may be decontrolled may be exercised only by, or with the permission of, the individual (or office) who made the original determination. The document shall indicate the name and organization of the individual removing the document from the SGI-M category and the date of the removal. Other persons who have the document in their possession should be notified of the decontrolling of the document.

Reproduction of Matter Containing SGI-M

SGI-M may be reproduced to the minimum extent necessary consistent with need without permission of the originator. Newer digital copiers which scan and retain images of documents represent a potential security concern. If the copier is retaining any information in memory, the copier cannot be connected to a network. It should also be placed in a location that is cleared and controlled for the authorized processing of SGI-M information. Different copiers have different capabilities, including some which come with features that allow the memory to be erased. Each copier would have to be examined from a physical security perspective.

Use of Automatic Data Processing (ADP) Systems

SGI-M may be processed or produced on an ADP system provided that the system is assigned to the licensee's or contractor's facility and requires the use of an entry code/password for access to stored information. Licensees must process this information in a computing environment that has adequate computer security controls in place to prevent unauthorized access to the information. An ADP system is defined here as a data processing system having the capability of long term storage of information. Word processors such as typewriters are not subject to the requirements as long as they do not transmit information off-site. (Note: if SGI-M is produced on a typewriter, the ribbon must be removed and stored in the same manner as other SGI-M information or media.) The basic objective of these restrictions is to prevent access and retrieval of stored SGI-M by unauthorized individuals, particularly from remote terminals. Specific files containing SGI-M will be password protected to preclude access by an unauthorized individual. SGI-M 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 NIST has validated as conforming to Federal Information Processing Standards (FIPS). SGI-M files shall be properly labeled as “**Safeguards Information - Modified Handling**” and saved to removable media and stored in a locked file drawer or cabinet. 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>.

Telecommunications

SGI-M 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 information useful to a potential adversary. Infrequent or non-repetitive telephone conversations regarding a physical security plan or program are permitted provided that the discussion is general in nature.

Individuals should use care when discussing SGI-M at meetings or in the presence of others to ensure that the conversation is not overheard by persons not authorized access. Transcripts, tapes or minutes of meetings or hearings that contain SGI-M shall be marked and protected in accordance with these requirements.

Destruction

Documents containing SGI-M must be destroyed when no longer needed. They 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 are considered completely destroyed.

Attachment B

Trustworthiness and Reliability Requirements for Individuals Handling Safeguards Information

Licensees shall document the basis for concluding that there is reasonable assurance that individuals granted access to safeguards information or who are placed in positions where they could facilitate access to the regulated material are trustworthy and reliable, and do not constitute an unreasonable risk for malevolent use of the regulated material.

The trustworthiness, reliability, and verification of an individual's true identity shall be determined based on a background investigation. The background investigation shall address at least the past three (3) years, and, as a minimum, include a local criminal history check (unless local or State laws prohibit local criminal history checks of current employees), verification of employment history, education, employment eligibility, and personal references. If an individual's employment has been less than the required three (3) year period, educational references may be used in lieu of employment history.

The licensee's background investigation requirements may be satisfied for an individual that has an active Federal security clearance.