ORIMDNRCOOOZ) or, where practicable, other fingerprint records for each individual seeking access to Safeguards Information, to the Director of the Division of Facilities and Security, marked for the attention of the Division's Criminal History Check Section. Copies of these forms may be obtained by writing the Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, by calling (301) 415–5877, or by e-mail to *forms@nrc.gov*. Practicable alternative formats are set forth in 10 CFR part 73.4. The Licensee shall establish procedures to ensure that the quality of the fingerprints taken results in minimizing the rejection rate of fingerprint cards due to illegible or incomplete cards.

The NRC will review submitted fingerprint cards for completeness. Any Form FD–258 fingerprint record containing omissions or evident errors will be returned to the Licensee for corrections. The fee for processing fingerprint checks includes one re-submission if the initial submission is returned by the FBI because the fingerprint impressions cannot be classified. The one free re-submission must have the FBI Transaction Control Number reflected on the re-submission. If additional submissions are necessary, they will be treated as initial submittals and will require a second payment of the processing fee.

Fees for processing fingerprint checks are due upon application. Licensees shall submit payment with the application for processing fingerprints by corporate check, certified check, cashier's check, money order, or electronic payment, made payable to ''U.S. NRC.'' [For guidance on making electronic payments, contact the Facilities Security Branch, Division of Facilities and Security, at (301) 415–7404]. Combined payment for multiple applications is acceptable. The application fee (currently $27) is the sum of the user fee charged by the FBI for each fingerprint card or other fingerprint record submitted by the NRC on behalf of a Licensee, and an NRC processing fee, which covers administrative costs associated with NRC handling of Licensee fingerprint submissions. The Commission will directly notify Licensees who are subject to this regulation of any fee changes.

The Commission will forward to the submitting Licensee all data received from the FBI as a result of the Licensee's application(s) for criminal history records checks, including the FBI fingerprint record.

Right To Correct and Complete Information

Prior to any final adverse determination, the Licensee shall make available to the individual the contents of any criminal records obtained from the FBI for the purpose of assuring correct and complete information. Written confirmation by the individual of receipt of this notification must be maintained by the Licensee for a period of one (1) year from the date of the notification. If, after reviewing the record, an individual believes that it is incorrect or incomplete in any respect and wishes to change, correct, or update the alleged deficiency, or to explain any matter in the record, the individual may initiate challenge procedures. These procedures include either direct application by the individual challenging the record to the agency (i.e., law enforcement agency) that contributed the questioned information, or direct challenge as to the accuracy or completeness of any entry on the criminal history record to the Assistant Director, Federal Bureau of Investigation Identification Division, Washington, DC 20537–9700 (as set forth in 28 CFR Part 16.30 through 16.34). In the latter case, the FBI forwards the challenge to the agency that submitted the data and requests that agency to verify or correct the challenged entry. Upon receipt of an official communication directly from the agency that contributed the original information, the FBI Identification Division makes any changes necessary in accordance with the information supplied by that agency. The Licensee must provide at least ten (10) days for an individual to initiate an action challenging the results of an FBI criminal history records check after the record is made available for his/her review. The Licensee may make a final SGI access determination based upon the criminal history record only upon receipt of the FBI's ultimate confirmation or correction of the record. Upon a final adverse determination on access to SGI, the Licensee shall provide the individual its documented basis for denial. Access to SGI shall not be granted to an individual during the review process.

Protection of Information

1. Each Licensee who obtains a criminal history record on an individual pursuant to this Order shall establish and maintain a system of files and procedures for protecting the record and the personal information from unauthorized disclosure.

2. The Licensee may not disclose the record or personal information collected and maintained to persons other than the subject individual, his/her representative, or to those who have a need to access the information in performing assigned duties in the process of determining access to Safeguards Information. No individual authorized to have access to the information may re-disseminate the information to any other individual who does not have a need-to-know.

3. The personal information obtained on an individual from a criminal history record check may be transferred to another Licensee if the Licensee holding the criminal history record check receives the individual's written request to re-disseminate the information contained in his/her file, and the gaining Licensee verifies information such as the individual's name, date of birth, Social Security number, sex, and other applicable physical characteristics for identification purposes.

4. The Licensee shall make criminal history records, obtained under this section, available for examination by an authorized representative of the NRC to determine compliance with the regulations and laws.

5. The Licensee shall retain all fingerprint and criminal history records received from the FBI, or a copy if the individual's file has been transferred, for three (3) years after termination of employment or determination of access to SGI (whether access was approved or denied). After the required three (3) year period, these documents shall be destroyed by a method that will prevent reconstruction of the information in whole or in part.

[FR Doc. E7–23364 Filed 11–30–07; 8:45 am]
BILLING CODE 7590–01–P

NUCLEAR REGULATORY COMMISSION

[EA–07–251]

In the Matter of All Licensees Identified in Attachment 1 and All Other Persons Who Obtain Safeguards Information Described Herein; Order Imposing Requirements for the Protection of Certain Safeguards Information (Effective Immediately)

I

The Licensee, identified in Attachment 1[1] to this Order, holds a license issued in accordance with the Atomic Energy Act of 1954, as amended, (AEA) by the U.S. Nuclear Regulatory Commission (NRC or Commission),

[1] Attachment 1 contains sensitive information and will not be released to the public.

authorizing it to possess and transfer items containing radioactive material quantities of concern. The NRC intends to issue security Orders to this licensee in the near future. The Order will require compliance with specific compensatory measures to enhance the security for large panoramic irradiators. The Commission has determined that these documents will contain Safeguards Information, will not be released to the public, and must be protected from unauthorized disclosure. Therefore, the Commission is imposing the requirements, as set forth in Attachments 2 and 3 to this Order and in Order EA–07–252, 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.

II

The Commission has broad statutory authority to protect and prohibit the unauthorized disclosure of Safeguards Information. Section 147 of the AEA grants the Commission explicit authority to ''* * * issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information* * *.'' This authority extends to information concerning the security measures for the physical protection of special nuclear material, source material, and byproduct material. 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 2 and 3 to this Order. The Commission hereby provides notice that it intends to treat violations of the requirements contained in Attachments 2 and 3 to this Order 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 the need to know the information, are considered to be trustworthy and reliable, and meet the requirements of Order EA–07–252. 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 2 and 3 to this Order. 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, or maintain and implement their own acceptable policies and procedures. The Licensee remains responsible for the conduct of their contractors. The policies and procedures necessary to ensure compliance with applicable requirements contained in Attachments 2 and 3 to this Order must address, at a minimum, the following: The general performance requirement that each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure; protection of Safeguards Information at fixed sites, in use and in storage, and while in transit; correspondence containing Safeguards Information; access to Safeguards Information; preparation, marking, reproduction and destruction of documents; external transmission of documents; use of automatic data processing systems; removal of the Safeguards Information category; the need-to-know the information; and background checks to determine access to the information.

In order to provide assurance that the Licensee is implementing prudent measures to achieve a consistent level of protection to prohibit the unauthorized disclosure of Safeguards Information, the Licensee shall implement the requirements identified in Attachments 2 and 3 to 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 81, 147, 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 32, 10 CFR part 35, and 10 CFR part 70, IT IS HEREBY ORDERED, EFFECTIVE IMMEDIATELY, THAT ALL LICENSEES IDENTIFIED IN ATTACHMENT 1 TO THIS ORDER AND ALL OTHER PERSONS WHO PRODUCE, RECEIVE, OR ACQUIRE THE ADDITIONAL SECURITY MEASURES IDENTIFIED ABOVE (WHETHER DRAFT OR FINAL) OR ANY RELATED SAFEGUARDS INFORMATION SHALL COMPLY WITH THE REQUIREMENTS OF ATTACHMENTS 2 AND 3 TO THIS ORDER.

The Director, Office of Federal and State Materials and Environmental Management Programs, may, in writing, relax or rescind any of the above conditions upon demonstration of good cause by the licensee.

IV

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 within twenty (20) days of the date of this Order. In addition, the Licensee and any other person adversely affected by this Order may request a hearing of this Order within twenty (20) days of the date of the Order. Where good cause is shown, consideration will be given to extending the time to request a hearing. A request for extension of time must be made, in writing, to the Director, Office of Federal and State Materials and Environmental Management Programs, 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. If the answer includes a request for a hearing, it shall, under oath or affirmation, specifically set forth the matters of fact and law on which the Licensee relies and the reasons as to why the Order should not have been issued. If a person other than the Licensee requests a hearing, that person shall set forth with particularity the manner in which his interest is adversely affected by this Order and shall address the criteria set forth in 10 CFR 2.309(d).

A request for a hearing must be filed in accordance with the NRC E-Filing

[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 of Energy 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.

rule, which became effective on October 15, 2007. The E-Filing Final Rule was issued on August 28, 2007, (72 Fed. Reg. 49,139). The E-Filing process requires participants to submit and serve documents over the internet or, in some cases, to mail copies on electronic optical storage media. Participants may not submit paper copies of their filings unless they seek a waiver in accordance with the procedures described below.

To comply with the procedural requirements associated with E-Filing, at least five (5) days prior to the filing deadline the requestor must contact the Office of the Secretary by e-mail at *HEARINGDOCKET@NRC.GOV,* or by calling (301) 415–1677, to request (1) a digital ID certificate, which allows the participant (or its counsel or representative) to digitally sign documents and access the E-Submittal server for any NRC proceeding in which it is participating; and/or (2) creation of an electronic docket for the proceeding (even in instances when the requestor (or its counsel or representative) already holds an NRC-issued digital ID certificate). Each requestor will need to download the Workplace Forms Viewer™ to access the Electronic Information Exchange (EIE), a component of the E-Filing system. The Workplace Forms Viewer™ is free and is available at *http://www.nrc.gov/site-help/e-submittals/install-viewer.html.* Information about applying for a digital ID certificate also is available on NRC's public Web site at *http://www.nrc.gov/site-help/e-submittals/apply-certificates.html.*

Once a requestor has obtained a digital ID certificate, had a docket created, and downloaded the EIE viewer, it can then submit a request for a hearing through EIE. Submissions should be in Portable Document Format (PDF) in accordance with NRC guidance available on the NRC public Web site at *http://www.nrc.gov/site-help/e-submittals.html.* A filing is considered complete at the time the filer submits its document through EIE. To be timely, electronic filings must be submitted to the EIE system no later than 11:59 p.m. Eastern Time on the due date. Upon receipt of a transmission, the E-Filing system time-stamps the document and sends the submitter an e-mail notice confirming receipt of the document. The EIE system also distributes an e-mail notice that provides access to the document to the NRC Office of the General Counsel and any others who have advised the Office of the Secretary that they wish to participate in the proceeding, so that the filer need not serve the document on those participants separately. Therefore, any others who wish to participate in the proceeding (or their counsel or representative) must apply for and receive a digital ID certificate before a hearing request is filed so that they may obtain access to the document via the E-Filing system.

A person filing electronically may seek assistance through the ''Contact Us'' link located on the NRC Web site at *http://www.nrc.gov/site-help/e-submittals.html* or by calling the NRC technical help line, which is available between 8:30 a.m. and 4:15 p.m., Eastern Time, Monday through Friday. The help line number is (800) 397–4209 or locally, (301) 415–4737.

Participants who believe that they have good cause for not submitting documents electronically must file a motion, in accordance with 10 CFR 2.302(g), with their initial paper filing requesting authorization to continue to submit documents in paper format. Such filings must be submitted by (1) first class mail addressed to the Office of the Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001, Attention: Rulemaking and Adjudications Staff; or (2) courier, express mail, or expedited delivery service to the Office of the Secretary, Sixteenth Floor, One White Flint North, 11555 Rockville, Pike, Rockville, Maryland, 20852, Attention: Rulemaking and Adjudications Staff. Participants filing a document in this manner are responsible for serving the document on all other participants. Filing is considered complete by first-class mail as of the time of deposit in the mail, or by courier, express mail, or expedited delivery service upon depositing the document with the provider of the service.

Documents submitted in adjudicatory proceedings will appear in NRC's electronic hearing docket which is available to the public at *http://ehd.nrc.gov/EHD_Proceeding/home.asp,* unless excluded pursuant to an order of the Commission, an Atomic Safety and Licensing Board, or a Presiding Officer. Participants are requested not to include personal privacy information, such as social security numbers, home addresses, or home phone numbers in their filings. With respect to copyrighted works, except for limited excerpts that serve the purpose of the adjudicatory filings and would constitute a Fair Use application, Participants are requested not to include copyrighted materials in their works.

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 requesting 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 ground 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 this 20th day of November 2007.

For The Nuclear Regulatory Commission.

Charles L. Miller,

Director, Office of Federal and State Materials and Environmental Management Programs.

Attachment 1: List of Applicable Materials Licensees Redacted

Attachment 2: Modified Handling Requirements for the Protection of Certain Safeguards Information (SGI–M)

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 would fall under this requirement if they possess facility 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 these 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 should 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:

A. An employee, agent, or contractor of an applicant, a licensee, the Commission, or the United States Government;

B. A member of a duly authorized committee of the Congress;

C. The Governor of a State or his designated representative;

D. 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;

E. A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies; or

F. 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.

G. 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 these individuals. 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 nationwide overnight service with computer tracking features, U.S. 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 each 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 SGI–M 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 are encouraged to 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 SGI–M. Word processors such as typewriters are not subject to the requirements as long as they do not transmit information offsite. (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. The National Institute of Standards and Technology (NIST) maintains a listing of all validated encryption systems at *http://csrc.nist.gov/cryptval/1401/1401val.htm*. 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.

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 insure 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 should 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 would be considered completely destroyed.

Attachment 3: Trustworthiness and Reliability Requirements for Individuals Handling Safeguards Information

Trustworthiness and Reliability Requirements for Individuals Handling Safeguards Information

In order to ensure the safe handling, use, and control of information designated as Safeguards Information, each licensee shall control and limit access to the information to only those individuals who have established the need-to-know the information, and are considered to be trustworthy and reliable. Licensees shall document the basis for concluding that there is reasonable assurance that individuals granted access to Safeguards Information are trustworthy and reliable, and do not constitute an unreasonable risk for malevolent use of the information.

The Licensee shall comply with the requirements of this attachment:

1. The trustworthiness and reliability of an individual shall be determined based on a background investigation:

(a) The background investigation shall address at least the past three (3) years, and, at a minimum, include verification of employment, education, and personal references. The licensee shall also, to the extent possible, obtain independent information to corroborate that provided by the employee (i.e., seeking references not supplied by the individual).

(b) 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.

2. The licensee shall retain documentation regarding the trustworthiness and reliability of individual employees for three years after the individual's employment ends.

[FR Doc. E7–23366 Filed 11–30–07; 8:45 am]

BILLING CODE 7590–01–P

OFFICE OF MANAGEMENT AND BUDGET

2007 List of Designated Federal Entities and Federal Entities

AGENCY: Office of Management and Budget.

ACTION: Notice.

SUMMARY: As required by the Inspector General Act of 1978, as amended (IG Act), this notice provides a list of Designated Federal Entities and Federal Entities.

FOR FURTHER INFORMATION CONTACT: Audrey Duchesne, Office of Federal Financial Management, Office of Management and Budget, telephone (202) 395–3993.

SUPPLEMENTARY INFORMATION: This notice provides the 2007 List of Designated Federal Entities and Federal Entities which, under the IG Act, the Office of Management and Budget (OMB) is required to publish annually. The previous list was published in the **Federal Register** on July 13, 2006 (71 FR 39691). This list is also posted on the OMB Web site at *http://www.whitehouse.gov/omb.* The Designated Federal Entities have been updated to reflect the: (1) Addition of Amtrak's statutory name, National Railroad Passenger Corporation; (2) addition of the Postal Regulatory Commission and its entity head as the Chairman to reflect the 2006 amendment to section 8G(a)(2) of the Inspector General (IG) Act (5 U.S.C. App. 3) by section 603(b) of the Postal Accountability and Enhancement Act (Pub. L. 109–435 (Dec. 20, 2006); 39 U.S.C. 504; and (3) change in the title of the Denali Commission's entity head from Chairperson to Federal Cochairperson for consistency with its enabling statute (42 U.S.C. 3121 note). The Federal Entities have been updated to reflect the: (1) Change of the Armed Forces Retirement Home entity head from Board of Directors to Chief Operating Officer consistent with the 2001 amendment of the Armed Forces Retirement Home Act of 1991 ((Pub. L. 101–510 Div. A, Tit. XV (Nov. 5, 1990); 24 U.S.C. 401 *et seq.*) by Sect. 1403 of Pub. L. 107–107 (Dec. 28, 2001), which established the Chief Operating Officer as the head, subject to the authority, direction and control of the Secretary of Defense; and (2) deletion of the National Veterans Business Development Corporation established under 15 U.S.C. 657c(a) (and its entity head as the Chairperson) because the Corporation is a private entity that did not receive any appropriations in fiscal year 2007 and will likely not receive any in fiscal year 2008.

The list is divided into two groups: Designated Federal Entities and Federal Entities. Designated Federal Entities are listed in the IG Act, except for those agencies that have ceased to exist or that have been deleted from the list. The Designated Federal Entities are required to establish and maintain Offices of Inspector General to: (1) Conduct and supervise audits and investigations relating to programs and operations; (2) promote economy, efficiency, and effectiveness of, and to prevent and detect fraud and abuse in such programs and operations; and (3) provide a means of keeping the entity head and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for, and progress of, corrective actions.

Section 8G(a)(1) of the IG Act defines a ''Federal entity'' as: Any Government corporation (within the meaning of section 103(1) of title 5, United States Code), any Government-controlled corporation (within the meaning of section 103(2) of such title), or any other entity in the Executive Branch of the Government, or any independent regulatory agency, but does not include:

(1) An establishment (as defined in section 11(2) of this Act or part of an establishment;

(2) A designated Federal entity [as defined in section 8G(a)(2) of the Act] or part of a designated Federal entity;

(3) The Executive Office of the President;

(4) The Central Intelligence Agency;