U.S. NUCLEAR REGULATORY COMMISSION April 2011

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 5.79

(Draft was issued as DG-5034, dated August 2009)
(New Regulatory Guide)

PROTECTION OF SAFEGUARDS INFORMATION

A. INTRODUCTION

This guide describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use in implementing the general performance requirements for the protection of Safeguards Information (SGI), as defined in Title 10 of the *Code of Federal Regulations*, Part 73 (10 CFR Part 73), "Physical Protection of Plants and Materials" (Ref. 1). Except where specifically stated, the guidance in this regulatory guide should be interpreted as applying to both SGI and SGI-M (SGI with the designation or marking "Safeguards Information-Modified Handling") requirements. This guide applies to all licensees, certificate holders, applicants, or other persons who produce, receive, or acquire SGI or SGI-M. It is intended to assist them in establishing an information protection system that addresses (1) information to be protected, (2) conditions for access and maintenance of the records associated with the access granting process, (3) protection while in use or storage, (4) preparation and marking of documents or other matter, (5) reproduction of matter containing SGI, (6) external transmission of documents and material, (7) processing of SGI on electronic systems, (8) removal from the SGI category, and (9) destruction of matter containing SGI.

In 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," the NRC requires, in part, that each licensee, certificate holder, applicant, or other person who produces, receives, or acquires SGI ensure that it is protected against unauthorized disclosure. The regulations in 10 CFR 73.21(a)(i) and (ii) require the establishment, implementation, and maintenance of an information protection system that includes the applicable measures for SGI specified in 10 CFR 73.22,

---

The NRC issues regulatory guides to describe and make available to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public.

Regulatory guides are issued in 10 broad divisions—1, Power Reactors; 2, Research and Test Reactors; 3, Fuels and Materials Facilities; 4, Environmental and Siting; 5, Materials and Plant Protection; 6, Products; 7, Transportation; 8, Occupational Health; 9, Antitrust and Financial Review; and 10, General.

Electronic copies of this guide and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/ doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML103270219. The regulatory analysis may be found in ADAMS under Accession No. ML103270227.

"Protection of Safeguards Information: Specific Requirements," or 10 CFR 73.23, "Protection of SafeguardsInformation—Modified Handling: Specific Requirements."

This regulatory guide contains information collection requirements covered by 10 CFR Part 73 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number. The NRC has determined that this regulatory guide is not a major rule as designated by the Congressional Review Act and has verified this determination with OMB.

B. DISCUSSION

SGI is a special category of sensitive unclassified information required to be protected from unauthorized disclosure under Section 147 of the Atomic Energy Act of 1954, as amended (AEA) (42 U.S.C. 2169) (Ref. 2). Although SGI is considered to be sensitive unclassified information, it is handled and protected more like classified national security information than like other sensitive unclassified information (e.g., privacy and proprietary information). The NRC has issued regulations in 10 CFR Part 73 setting forth the requirements for the protection of SGI. These requirements apply to SGI in the hands of any person, whether or not a licensee of the Commission, who produces, receives, or acquires SGI. An individual's access to SGI requires both a valid "need to know" and a determination that the individual in question is trustworthy and reliable based on an appropriate background check.

The Commission has the authority, under Section 147 of the AEA, to designate, by regulation or Order, other types of information as SGI. For example, Section 147a.(2) of the AEA allows the Commission to designate as SGI a licensee's or applicant's detailed security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material in quantities determined by the Commission to be significant to public health and safety or the common defense and security. By Order, the Commission has imposed SGI handling requirements on certain categories of these licensees. An example is Order EA 03-199, "Order Imposing Requirements for Protection of Certain Safeguards Information," issued November 25, 2003 (Ref. 3), to certain materials licensees.

On February 11, 2005, the NRC published a proposed rule (70 FR 7196) to amend its regulations governing the handling of SGI and to create a new category of protected information labeled "Safeguards Information-Modified Handling." SGI-M refers to SGI with handling requirements that are modified somewhat because of the lower risk posed by unauthorized disclosure of the information. The SGI-M protection requirements apply to certain security-related information regarding quantities of source, byproduct, and special nuclear materials for which the harm caused by unauthorized disclosure of information would be less than that caused by the disclosure of other SGI.

Subsequently, Congress enacted the Energy Policy Act of 2005 (EPAct) (Public Law No. 109-58, 119 Stat. 594) (Ref. 4). Section 652 of the EPAct amended Section 149 of the AEA to require fingerprinting and criminal history records checks for a broader class of individuals. Before the EPAct, the NRC's fingerprinting authority was limited to requiring licensees and applicants for a license to operate a nuclear power reactor under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," (Ref. 5) to fingerprint individuals before granting them access to SGI. The EPAct expanded the NRC's authority to require fingerprinting of individuals associated with other types of activities before granting them access to SGI. The EPAct preserved the Commission's authority in Section 149 of the AEA to relieve by rule certain persons from the fingerprinting, identification, and criminal history records checks required for access to SGI.

Categories of individuals relieved from elements of the background check are listed in 10 CFR 73.59, "Relief from Fingerprinting, Identification and Criminal History Records Checks, and Other Elements of Background Checks for Designated Categories of Individuals." The Commission based these exemptions on its findings that interrupting the individuals' access to SGI to perform fingerprinting and criminal history records checks (1) would harm vital inspection, oversight, planning, and enforcement functions, (2) would impair communications among the NRC, its licensees, and first responders in the event of an imminent security threat or other emergency, and (3) could strain the Commission's cooperative relationships with its international counterparts and might delay needed exchanges of information to the detriment of current security initiatives, both at home and abroad. The NRC published the final rule regarding relief from the fingerprinting and criminal history records check requirements in the *Federal Register* (71 FR 33989) on June 13, 2006 (Ref. 6). That final rule was necessary to avoid disruption of the Commission's information-sharing activities during the interim period while the Commission completed the overall revision of the SGI-related regulations in 10 CFR 73.21, 73.22 and 73.23. As part of the final SGI rulemaking, the Commission made additional revisions to10 CFR 73.59, which are now reflected in the rule. The cumulative efforts of the staff to increase the protection requirements associated with SGI and SGI-M culminated in writing and publication of the final rule. The rule, Protection of Safeguards Information, was published in the *Federal Register* on October 24, 2008 (73 FR 63546) (Ref. 7). As stated in the rule, the purpose of the rulemaking was, in part, to "implement generally applicable requirements for SGI that are similar to requirements imposed by the Orders."

Stakeholders should also note that the final SGI rule does not automatically supersede the existing SGI Orders. Licensees who received Orders regarding the protection of SGI or requiring fingerprinting for access to SGI are still subject to the requirements of those Orders until the Commission determines otherwise. Though the NRC's intent is that all SGI protection requirements will ultimately be embodied in regulations, the Orders currently contain several provisions not included in the final SGI rule that the NRC continues to view as an essential part of the agency's SGI protection requirements. An example is the requirement for a "reviewing official." The NRC determined during the rulemaking that incorporating all of those additional requirements into the new SGI rule could have adversely affected the rulemaking process and, at a minimum, would have further delayed publication of a final rule.

Because the NRC considers these requirements in the Orders important to ensuring adequate protection, the Orders will remain in effect until the Commission decides to relax the requirements of the Orders in whole or in part. Until that time, Order recipients are obliged to comply with both the rule and the Order. In those few instances where there is a variance between the rule and the Orders, licensees and other recipients of those Orders are required to comply with the more stringent requirement whether in the rule or the applicable Order.

For example, though the Orders require only a need to know and a criminal history records check as a prerequisite for access to SGI, the SGI rule requires a trustworthiness and reliability determination based on a background check (which includes a criminal history records check). Therefore, the more stringent access requirements of the rule apply for SGI access determinations. In contrast, the Orders are more stringent with regard to requiring an NRC-approved reviewing official; thus, Order recipients are also obligated to maintain an NRC-approved reviewing official, as required by the Order. Licensees and others should note that the completion of the "background check" required for access to SGI does not satisfy the "background investigation" requirement for unescorted access authorization to nuclear power plants. The Commission will ultimately decide when and by what means it will relax the Orders and will then notify licensees and others accordingly.

C. REGULATORY POSITION

1. Performance Requirements

a. Each licensee, certificate holder, applicant, or other person (hereafter referred to as "licensee") who produces, receives, or acquires SGI (including SGI-M) shall ensure that it is protected against unauthorized disclosure, in accordance with 10 CFR 73.21(a).

b. Regulations in 10 CFR 73.21(a)(1)(i) require licensees to establish, implement, and maintain an information protection system for the protection of SGI. The system should do the following:

(1) be formally documented to reflect intended program activities and organizational commitments regarding the local procedures that are required by 10 CFR 73.22(b) through (i) or 10 CFR 73.23(b) through (i),

(2) identify key personnel with responsibilities for implementation,

(3) establish an independent audit of the protection system on a 12-month cycle,

(4) identify the process for authorizing SGI access to third parties (e.g., contractors, consultants),

(5) establish a system for SGI-related records review and retention,

(6) establish procedures to describe information security violations and appropriate corrective actions, and

(7) provide training to individuals authorized access to SGI on the procedures and guidance for tasks associated with the identification and protection of SGI.

c. Any person, whether or not a licensee of the NRC, who produces, receives, or acquires SGI is subject to the requirements of 10 CFR 73.21(a)(1) .

If information is thought to be SGI, but not marked as such, and it is not clear whether the requirements of 10 CFR 73.22 or 10 CFR 73.23 apply, the possessor should treat the information in the most conservative manner by applying the protection provisions of 10 CFR 73.22(b) through (i) (excluding 10 CFR 73.22(d)), and obtain clarification from the originator as soon as practicable, so that the information can be protected at the appropriate level. If it is determined that the information is SGI, the appropriate SGI markings must be applied to the document as prescribed by 10 CFR 73.22(d) and 10 CFR 73.23(d). Additionally, the possessor should initiate an inquiry if the information in question is believed to have been viewed or otherwise obtained by personnel not authorized access to SGI.

d. Licensees should inform Federal, State, and local law enforcement agencies of the SGI requirements before transferring SGI to them, so that these agencies are fully aware of the protection requirements for SGI and the potential for civil and criminal sanctions against any person who discloses SGI in an unauthorized manner. These law enforcement agencies are presumed to meet the information protection requirements of 10 CFR 73.21(a)(1).

The conditions for transfer of SGI to a third party (e.g., need to know) would still apply to law enforcement agencies. Before sharing or providing third-party access to SGI with an authorized recipient, the possessor is responsible for ensuring that the SGI will be properly protected. For example, the possessor could fulfill this responsibility, before sharing the SGI, through the process of providing a copy of this regulatory guide or by obtaining written or oral confirmation that the recipient understands the protection and handling requirements applicable to SGI.

2. Specific Requirements

a. Information , described in 10 CFR 73.22(a) and 10 CFR 73.23(a), may be designated as either SGI or SGI-M, as appropriate.

b. Information on security measures is usually not considered SGI if the information is legitimately in the public domain. Also, absent extraordinary circumstances, information that is placed in the public domain by a person, not affiliated with a NRC regulated entity and who otherwise has no knowledge that the information has been designated as SGI, is typically not treated as SGI nor made subject to the NRC's SGI protection requirements.

Occasionally, industry-wide weaknesses or new areas of concern may be identified that affect licensee programs. The response to these developments by the NRC or licensees may be designated as SGI if the information is required to address an industry-wide or individual licensee weakness in a program for the physical protection of special nuclear material or radioactive materials. As licensees complete upgrades to address such weaknesses, they may consider removing these protective measures from the SGI category. Sometimes, a weakness may be corrected at one facility but not at other facilities, and such information could still be valuable to a potential adversary. Licensees shall take care to prevent any document or other matter that is decontrolled from disclosing SGI in some other form or from being combined with other unprotected information to disclose SGI in accordance with 10 CFR 73.22(h) and 10 CFR 73.23(h). Information of a general nature and not specific to a particular facility is usually not SGI unless, for example, it concerns studies of the impacts of postulated security events on nuclear facilities or radioactive materials or it discloses generic consequences to a class of facilities or material users. Normal engineering or construction drawings showing the location of safety-related equipment, that do not otherwise identify the equipment as vital for purposes of physical protection, are not SGI. The specificity of the information and its usefulness in defeating security measures at a particular facility increases the likelihood that it will be advantageous to an adversary and must be designated SGI in accordance with 10 CFR 73.22(a)(1)(xii) and 10 CFR 73.23(a)(1)(x). The overall measure for the designation of SGI is the usefulness of the information (security or otherwise) to an adversary in planning or attempting a malevolent act.

c. General information on local law enforcement, such as total complement and shift size, which is legitimately in the public domain, is not SGI. However, detailed local law enforcement response information relating to a particular licensed facility may be SGI.

3. Conditions for Access

a. Access to SGI requires that an individual have a need to know, have undergone a Federal Bureau of Investigation (FBI) criminal history records check, and be deemed trustworthy and reliable based on a favorably adjudicated background check, as prescribed by 10 CFR 73.22(b)(1), 73.22(b)(2), 73.23(b)(1), and 73.23(b)(2).

The trustworthiness and reliability determination is based on verification of identity, employment history, education, criminal history records check, and appropriate reference checks, as defined by "background check" in 10 CFR 73.2, "Definitions." The verification of a person's stated level of education, or stated period of time for which education was in lieu of employment, is considered a key attribute in determining a person's trustworthiness and reliability. With respect to references, as one of the elements of a background check as defined in 10 CFR 73.2, the rule does not differentiate between stated personal references and developed references. This is different from the requirements associated with completion of the background investigation. Licensees may use either personal references or developed references when collecting information to make a trustworthiness and reliability determination for access to SGI. This determination takes into account the results of the background check and the characteristics of the individual. There is no required scope of investigation for the background check, but an examination of at least the past 3 years of all elements of the background check should be sufficiently probative to support a trustworthiness and reliability determination.

b. The NRC has not established or endorsed any specific disqualifying criteria for the FBI criminal history records check nor for the information gleaned from the other elements of the background check. At a minimum, the criteria used to adjudicate the results of the FBI criminal history records check and other elements of the background check must not conflict with the prohibitive practices stated in 10 CFR 73.57(c) (Ref. 8). The regulation does not prescribe adjudication standards. However, licensees and others should use their best judgment and experience in determining which individuals are trustworthy and reliable and therefore suitable for access to SGI. The standards for determining trustworthiness and reliability should be consistent and sufficiently probative to be capable of supporting an individual trustworthiness and reliability determination.

c. The regulations contain no reinvestigation requirement for continuing access to SGI. However, the regulations at 10 CFR 73.22(b) and 10 CFR 73.23(b) require that persons with access to SGI be trustworthy and reliable, based on a background check. If a licensee, applicant, or certificate holder (responsible party) learns of information that would reasonably call into question the trustworthiness and reliability of an individual already authorized access to SGI or SGI-M, the responsible party should reevaluate the individual's access authorization.

d. Individuals possessing an active Federal security clearance require no additional fingerprinting or background check for access to SGI, as this clearance meets the fingerprinting requirement and other elements of the background check, as prescribed in 10 CFR 73.22(b)(1) and 10 CFR 73.23(b)(1). When relying on an existing active Federal security clearance to meet the SGI access requirements (excluding need to know), the licensee should obtain and maintain a record of official notification stating that the individual has such a clearance.

e. Persons possessing SGI access authorization at the time the final rule was published (October 24, 2008, Ref. 7) need not undergo additional fingerprinting for continued access to SGI. To meet the requirements of the rule, employees who have not been the subject of other elements of the new background check, such as employment history, educational history, and personal references, as prescribed in 10 CFR 73.22(b) and 10 CFR 73.23(b), would have to undergo a background check for those elements alone and, based on all of the information obtained, be found trustworthy and reliable, to continue to have access to SGI. Until all of those elements are completed, individuals must not have access to SGI in accordance with 10 CFR 73.22(b) and 10 CFR 73.23(b). This does not mean that individuals who have been subject to an equivalent background check (such as for unescorted access or for access to national security information) will have to undergo another background check for access to SGI.

f. For persons participating in an NRC adjudicatory proceeding, the originator of the SGI must make the need-to-know determination upon receipt of a request for access to the SGI as prescribed by 10 CFR 73.22(b)(4) and 10 CFR 73.23(b)(4). Where the information is in the possession of the originator and the NRC staff, whether in its original form or incorporated into another document or other matter by the recipient, the NRC staff will make the determination. In the event of a dispute regarding the need-to-know determination, the presiding officer of the proceeding will determine if the individual has the requisite need to know, as defined in 10 CFR 73.2.

g. The following individuals do not have to undergo fingerprinting, a criminal history records check, and other elements of the background check before being granted access to SGI, consistent with 10 CFR 73.59:

(1) an employee of the Commission or of the executive branch of the U.S. Government who has undergone fingerprinting for a prior U.S. Government criminal history check;

(2) a Member of Congress;

(3) an employee of a Member of Congress or a congressional committee who has undergone fingerprinting for a prior U.S. Government criminal history check (Ref. 9);

(4) The Comptroller General or an employee of the Government Accountability Office who has undergone fingerprinting for a prior U.S. Government criminal history records check;

(5) the Governor of a State or his or her designated State employee representative;

(6) a representative of a foreign government organization that is involved in planning for, or responding to, nuclear or radiological emergencies or security incidents for whom the Commission has approved access to SGI;

(7) Federal, State, or local law enforcement personnel;

(8) State Radiation Control Program Directors and State Homeland Security Advisors or their designated State employee representatives;

(9) Agreement State employees conducting security inspections on behalf of the NRC under an agreement executed under Section 274.i. of the AEA;

(10) representatives of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who have been certified by the NRC; and

(11) any agent, contractor, or consultant of the aforementioned persons who has undergone criminal history records and background checks equivalent to those required by 10 CFR 73.22(b) or 10 CFR 73.23(b).

The individuals described above are considered trustworthy and reliable by virtue of their position, or they have already undergone a background or criminal history check or its equivalent.

h. Consistent with 10 CFR 73.59(f), representatives of foreign governments are not subject to fingerprinting and criminal history checks. The phrase "a representative of a foreign government organization" may include more than employees of foreign governments. The phrase may encompass members of private industry, local first responders, vendors, law enforcement officials, or other individuals who have been designated by a foreign government organization involved in nuclear emergency planning or incident response to serve as foreign government representatives before the NRC.

i. Many licensees have been required by NRC Order to appoint an NRC-approved reviewing official. Those licensees who are not subject to such an Order should appoint a reviewing official to independently review the background check information and make a determination that the individual is trustworthy and reliable.

Section 149 of the AEA, as amended, requires that the Commission fingerprint any individual who is permitted unescorted access to a utilization facility, or certain radioactive material subject to regulation by the Commission, or access to SGI. The NRC does not have the authority to fingerprint any other classes of individuals. Therefore, the NRC has determined that the individual to be designated as a reviewing official must fall into one of these classes of individuals.

j. The reviewing official processing each individual requiring access to SGI and subject to the fingerprint provisions, shall fingerprint the individual, or ensure that the individual's fingerprints have been taken, and submit those fingerprints to the NRC for transmission to the FBI in accordance with 10 CFR 73.22(b) and 10 CFR 73.23(b).

The licensee should review the information received from the FBI and ensure that all elements of the background check are sufficiently addressed before initiating the adjudication process and making the trustworthiness and reliability determination. The NRC considers certain industry standards, such as those found in the applicable elements of the most recent NRC endorsed revision of Nuclear Energy Institute document NEI 03-01, "Nuclear Power Plant Access Authorization Program," (Ref. 10) to be an acceptable means for licensees to use when making a trustworthiness and reliability determination.

k. Licensees shall inform individuals requesting SGI access that their fingerprints will be used to obtain information about their criminal history and that they have the right to obtain or review the content of their record to ensure that correct and complete information is used during the adjudication process, as prescribed by 10 CFR 73.57(b)(3). Consistent with the requirements of 10 CFR 73.57(f)(5), licensees shall retain the fingerprint and criminal history records received from the FBI for a period of 1 year from the date that the individual's employment was terminated or that the individual was denied access to SGI. Additionally, licensees should also retain documented information used to support or deny the trustworthiness and reliability determination.

l. Each individual record of those requesting SGI access should contain the documentation that was relied on to make the SGI access determination. In those instances where the SGI access is denied, a brief explanation of the reason for the denial should also be made a part of the individual record. Licensees should consider employing a degree of reciprocity with respect to acknowledgment of recently adjudicated background checks from other licensees. In all instances (approval and disapproval), the individual record must be retained for 1 year after termination of employment or denial of SGI access, in accordance with 10 CFR 73.57(f)(5).

A licensee or licensee official shall not base a final determination to deny an individual access to SGI solely on information received from the FBI if it involves an arrest more than 1 year old for which there is no information on the disposition of the case, or an arrest that resulted in either a dismissal of the charge or an acquittal, in accordance with 10 CFR 73.57(c). Licensees should ensure that potentially disqualifying information obtained from confidential or unnamed sources is substantiated and documented, and such information should not be used as the sole basis to deny SGI access.

m. Each licensee that obtains an individual's criminal history record shall establish and maintain a system of files and procedures for protecting the record and the personal information from unauthorized disclosure, as prescribed by 10 CFR 73.57(f).

The licensee may not disclose the record or personal information collected and maintained to persons other than the subject individual, to his or her representative, or to those who have a need to access the information in performing assigned duties to determine access to SGI. No individual authorized to have access to the record may re-disseminate the information to any other individual who does not have a need to know, as prescribed by 10 CFR 73.57(f)(2).

The personal information obtained about an individual from a criminal history records check may be transferred to another licensee, in accordance with 10 CFR 73.57(f)(3), if the licensee possessing the information receives the individual's written request to re-disseminate the information contained in his or her file, and if the requesting licensee verifies that key information contained within the record, such as the individual's name, date of birth, social security number, and gender, is consistent with the proof of identification presented to the licensee and the physical characteristics of the individual.

4. Protection While in Use or Storage

a. While in use, matter containing SGI must be under the control of an individual authorized access to it, as prescribed by 10 CFR 73.22(c)(1) and 10 CFR 73.23(c)(1).

This requirement is satisfied if the SGI is attended by such an individual, even though the information is, in fact, not constantly being used. SGI within alarm stations, or rooms continuously occupied by SGI-authorized individuals, need not be stored in a locked security storage container.

b. SGI must be under the control of an authorized user, or be placed in a security storage container, as prescribed by 10 CFR 73.22(c)(2). Security storage containers used to house SGI must not have exterior markings that identify the content of the containers and must prevent access by individuals not authorized access to SGI, in accordance with 10 CFR 73.22(c)(2). Marking a locked security storage container to indicate that it contains SGI may draw unwarranted attention to it. The use of an open/close magnetic sign does not violate the requirements of the rule, because the magnetic sign does not reveal the contents of the security storage container.

c. SGI-M may be stored in a locked file drawer or cabinet when not in use. Like security storage containers used to house SGI, the container used to house SGI-M must not identify its content and must prevent access by individuals not authorized access to SGI-M, as prescribed by 10 CFR 73.23(c)(2). Encrypting SGI-M does not relieve an individual of his or her responsibility to place SGI-M in a locked file drawer or cabinet when it is not in use. The requirement for "in use" is satisfied if the matter is attended by SGI-M authorized individuals, even though the information is, in fact, not constantly being used.

d. The encryption of SGI for storage on hard drives or a removable storage medium does not relieve an individual of his or her responsibility to place SGI in a locked security storage container when it is not in use. Adequate storage of SGI may consist of any of the following:

(1) a steel filing cabinet equipped with a steel locking bar (located within a protected or controlled access area as defined in 10 CFR 73.2, and a three-position, changeable combination padlock approved by the U.S. General Services Administration (GSA); or

(2) a security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked "GSA-Approved Security Container" on the exterior of the top drawer or door; or

(3) a safe-deposit box (located within a bank); or

(4) a repository that, in the judgment of the NRC, would provide comparable physical protection.

Licensees and others that wish to obtain NRC approval for a repository that provides comparable physical protection, as referenced above, e.g. a container constructed of steel, housed within a controlled access room and equipped with steel locking bars and a three-position GSA approved padlock or similar container housed within a controlled access facility with supplemental security measures, should submit a request to the NRC through the Office of Nuclear Security and Incident Response.

e. The general control exercised over protected or controlled access areas are considered to meet the "under the control of" or "is attended by" requirement referenced in 10 CFR 73.22(c)(1) and 10 CFR (73.23)(c)(1). The primary consideration is to limit access only to those who have a need to know and to ensure continuous occupancy by SGI-authorized personnel. Some examples of SGI storage locations include, but are not limited to, the following:

(1) the above-mentioned alarm stations, guard posts, and guard ready-rooms;

(2) an engineering or drafting area, if visitors are escorted;

(3) certain nuclear power plant vital areas, such as the control room or security office;

(4) plant maintenance areas, if access is restricted; or

(5) administrative offices, such as for central records or purchasing, if visitors are escorted.
SGI that has been removed from the security storage container and is located in a continuously manned guard post or ready-room need not be locked in security storage containers. Similarly, guards or transport escorts may carry orders and response plans on a routine basis. Care should still be taken so that individuals, absent SGI access authority and a need to know, not gain access to the SGI.

f. Licensees should change the combination to the security storage container if compromise is suspected or if individuals who know the combination lose their need to know or access to SGI. Licensee that rely upon file drawers or cabinets to house SGI-M should consider lock replacement, lock rekeying or some other means to ensure information protection.
Changing the combination within 1 business day of an individual's loss of need to know or loss

of access to SGI helps to reduce the risk of inadvertent or unauthorized disclosure of SGI.

Each security storage container should have an associated record that is used to record its opening and closing. When fellow employees or guard force members conduct security container checks, the record becomes a valuable tool for determining how long a security storage container may have been left open and unattended. The Standard Form 702 can be used to capture the needed opening and closing data and should be considered for this purpose.

g. Licensees should discuss SGI only after reasonable efforts have been made to isolate the discussion from those without a need to know.

Licensees should ensure that rooms with walls that serve as barriers to exterior portions of the facility or to the discussion area itself are checked for sound attenuation, and if it is determined that the sound travels beyond the confines of the room, either the sound emanations should be mitigated or the SGI discussion should not take place.

5. Preparation and Marking

a. To indicate the presence of SGI, documents must be conspicuously marked at the top and bottom (preferably in a font larger than that used in the body of the document) with the words "SAFEGUARDS INFORMATION," as prescribed by 10 CFR 73.22(d)(1) or "SAFEGUARDS INFORMATION-MODIFIED HANDLING" as by 10 CFR 73.23(d)(1).

b. Only designated and trained individuals should have the authority to designate a document as SGI. The first page of SGI documents must contain the following information, in accordance with 10 CFR 73.22(d):

(1) the identification of the organization making the SGI designation,

(2) the name and title of the SGI designating official (person authorized to make an SGI determination),

(3) the date that the document or other matter was designated SGI, and

(4) an indication that unauthorized disclosure will be subject to civil and criminal penalties.

c. Licensees are not expected to go back and mark documents if a cover sheet was used for the required information instead of the first page of the document, as prescribed in 10 CFR 73.22(d)(1) and 10 CFR 73.23(d)(1).

Historical documents that are in storage need not be removed solely for the purpose of meeting the marking requirement. As those documents are removed from storage for use (i.e., transmittal, modification, or use as an attachment), they must be marked as required by the rule. If the first page of the document is the cover page, then the required markings would be conspicuously placed on the cover page. The rule makes no distinction with respect to the marking of electronic documents and hard-copy documents or other matter containing SGI. Electronic SGI documents must be marked as prescribed in 10 CFR 73.22(d)(1) and 10 CFR 73.23(d)(1).

d. To indicate that unauthorized disclosure is subject to civil and criminal penalties, as required by 10 CFR 73.22(d)(1)(iii) and 10 CFR 73.23(d)(1)(iii), licensees should consider placing the following text on the bottom (left side) of the document:

VIOLATION OF SECTION 147 OF THE ATOMIC ENERGY ACT, "SAFEGUARDS INFORMATION," IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES

e. When SGI has been removed from the security container, an SGI coversheet should be attached to the document. When entire file folders containing SGI are removed, they should be conspicuously marked, front and back, to indicate that they contain SGI. The file folder marking can be in the form of written or stamped text, or a coversheet can be attached to the file folder to meet the requirement for conspicuous marking. If a binder is used to store SGI, and the binder is stored in a manner that conceals the SGI marking, the spine of the binder should also be marked to indicate the presence of SGI.

f. When electronic removable storage media, charts, maps, or overhead slides contain SGI, each item must visibly indicate that SGI is contained therein. The associated markings (e.g., the designator's name, date, organization) must be placed on the media itself or on the accompanying cover or protective case in accordance with 10 CFR 73.22(d)(1) and 10 CFR 73.23(d)(1).

g. Transmittal documents that do not contain SGI or any other sensitive information but have an SGI enclosure or attachment must contain the name and title of the certifying official and the date that the information was designated as SGI in accordance with 10 CFR 73.22(d)(3) and 10 CFR 73.23(d)(3).

In addition, the sentence set forth in 10 CFR 73.22(d)(2) and 73.23(d)(2) should also be conspicuously placed at the bottom of the transmittal document when it does not otherwise contain sensitive information that warrants protection from unauthorized disclosure.

Every effort should be made to ensure that the transmittal document does not include SGI. However, when SGI or SGI-M is included in transmittal documents that are forwarded to the NRC, portion markings must be used to distinguish those portions of the transmittal document that contain SGI as prescribed by 10 CFR 73.22(d)(3) and 10 CFR 73.23(d)(3). When applying portion markings to a transmittal document containing SGI or SGI-M, the document marking requirements of 10 CFR 73.22(d) and 10 CFR 73.23(d) must be adhered to. Additionally, licensees and others should:

(1) place the acronym (SGI) or (SGI-M), as applicable to the portion's content, at the beginning of the sentence, section or paragraph.

(2) mark each subsection to a paragraph containing SGI or SGI-M, individually, to reflect the designation of information contained within that particular subsection.

6. Reproduction

a. Licensees may reproduce SGI to the minimum extent necessary consistent with need. Licensees must evaluate equipment used to reproduce SGI to ensure that unauthorized individuals cannot access SGI, in accordance with 10 CFR 73.22(e) and 10 CFR 73.23(e). The evaluation should consider the potential for retention of residual images on the copier.

b. Copier machines that have e-mail, fax, or remote diagnostic capabilities should not be used to reproduce SGI, nor should facsimile machines be used to reproduce SGI. Some copiers have memory capability and, for that reason, only designated copiers should be used to reproduce SGI. When memory-capable copiers are used to reproduce SGI, licensees must take steps to prevent unauthorized personnel (including copier maintenance personnel) from gaining access to SGI through retained memory, network connectivity, or remote diagnostics in accordance with 10 CFR 73.22(e) and 10 CFR 73.23(e). Copiers that have been designated for the reproduction of SGI must be clearly identified. When reproducing SGI, personnel should immediately clear paper jams and properly destroy unwanted documents.

7. External Transmission

a. Except under emergency or extraordinary conditions, as prescribed in 10 CFR 73.71, "Reporting of Safeguards Events," licensees shall limit telephone discussions involving SGI to NRC-approved secure voice communications.

NRC-approved secure voice communication equipment uses encryption that is compliant with Federal Information Processing Standard (FIPS) 140-2, or later. Those involved with the telecommunication should ensure that the SGI is protected from unauthorized disclosure by sound attenuation from within the discussion area, as well as from the area(s) immediately adjacent to the room or the area where the discussion is taking place.

b. When SGI is discussed at impromptu and informal discussions or meetings, it is not necessary to turn off cell phones. However, as a matter of standard practice, cellular telephones and other two-way communication devices should be turned off and/or not allowed within the meeting room at formally arranged meetings or discussions that involve SGI. Taking such a proactive position reduces the potential for an inadvertent transmission of SGI.

c. The rule contains no restriction on where SGI can be used or stored, but it is recommended that licensees not permit the use, handling, or storage of SGI from one's home or private residence. SGI should not be removed from a licensee's facility for the purpose of working from home because of the increased potential for inadvertent or unauthorized disclosure and the lack of adequate storage accommodations. When licensees grant authorization for SGI to be taken to a home or private residence for the purpose of accommodating business travel to or from the official storage location, licensees should emphasize that **the NRC's regulations on storage of SGI continue to apply** and that the authorization is limited and **is not intended** to permit the **long-term** use of, processing of, or review of SGI while at the home or private residence.

d. Individuals who arrange or participate in public hearings, conferences, or discussions involving SGI must do the following:

(1) ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed;

(2) indicate to participating personnel that the specific information they will receive is SGI and advise them of the protective measures required; and

(3) ensure that no discussion takes place that is audible or visible to persons not authorized access to the information.

e. Licensees should hold hearings, conferences, and discussions involving SGI within guarded or controlled areas, if practicable, and preferably at locations owned and controlled by NRC licensees.

(1) Conferences should be held outside guarded or controlled areas only when security management is consulted. That consultation should be accomplished for the purposes of obtaining the appropriate guidance for the physical protection of SGI.

(2) Transcripts of hearings and meeting minutes that contain SGI must be marked and protected, in accordance with 10 CFR 73.22(d)(4) and 10 CFR 73.23(d)(4).

f. When SGI is transmitted, the mode of transmission will dictate the procedures that should be followed.

In every case, before SGI is transmitted, the sender must verify that the intended recipient is someone that is authorized to access SGI and has a need to know. Licensees should follow the procedures listed below when transmitting SGI:

(1) Hand-carrying—Licensees should hand-carry SGI outside the facility only as a last resort, when other means of transmitting the information have failed or are not practicable. The SGI must be double-wrapped through the use of two opaque wrappers. The inner wrapper must be sealed and marked top and bottom, front and back, with the words "Safeguards Information" and be properly addressed (i.e., the address of the intended recipient), as prescribed by 10 CFR 73.22(f) and 10 CFR 73.23(f). A briefcase or other lockable or sealed opaque container may be used to meet the outer wrapper requirement. The outer wrapper must not indicate the sensitivity of the information contained therein.

(2) Mail—When SGI is mailed, two sealed opaque envelopes or containers must be used as prescribed by 10 CFR 73.22(f)(1) and 10 CFR 73.23(f)(1).

(a) The inner envelope or container must be marked top and bottom, front and back, with the words "Safeguards Information." The envelope or container must also be addressed to the intended recipient.

(b) Like the inner envelope or container, the outer envelope or container must be addressed to the intended recipient, but the outer envelope differs slightly in that a return address must be indicated and the outer envelope or container must have no markings to indicate that SGI is contained within.

(c) Licensees should also consider placing guidance to the postmaster beneath the return address. Guidance such as "POSTMASTER: Do Not Forward, Return to Sender" should be sufficient to ensure that the SGI is not forwarded to an address other than the one on the envelope or container.

(d) SGI may be transported by any commercial delivery company that provides service with computer-tracking features; by U.S. first class, registered, express, or certified mail; or by any individual authorized access under these requirements, as prescribed by 10 CFR 73.22(f)(2) and 10 CFR 73.23(f)(2). When express mail is used, a signature should be required. When interoffice mail systems or couriers are relied on to transport SGI from one office to another,

the package wrapping requirements prescribed by 10 CFR 73.22(f)(1) and 10 CFR 73.23(f)(1) remain applicable.

(3) Electronic transmission—Except under emergency or extraordinary conditions, SGI must be transmitted outside an authorized place of use or storage only by NRC-approved secure electronic devices, such as facsimiles or telephones. To meet the requirement for SGI transmission through electronic mail (i.e., use of the Internet), licensees must encrypt SGI, using any level of FIPS 140-2, or later, encryption on a stand-alone computer processing unit as prescribed by 10 CFR 73.22(f)(3).

(a) Encrypted SGI can be placed on a removable storage medium, transported to an Internet-connected computer, and embedded in an e-mail for transmission. Upon completion of the transmission, the licensee should take affirmative action to remove all traces of the encrypted SGI from the Internet-connected computer processing unit.

(b) Internet servers used to transmit the e-mail with the embedded encrypted SGI file are not expected to be purged of the encrypted file.

(c) Both the transmitter and the receiver must use information-handling processes to ensure protection of the SGI before and after transmission, as prescribed by 10 CFR 73.22(f)(3).

(d) Physical security events required to be reported pursuant to 10 CFR 73.71 are considered to be extraordinary conditions in accordance with 10 CFR 73.22(f)(3) and 10 CFR 73.23(f)(3).

FIPS 140-2, or later, encryption is an acceptable method to encrypt electronic files and is the only unclassified standard authorized for electronic transmission of SGI. Licensees may also use a higher level of encryption, such as that authorized for classified information.

8. Processing Safeguards Information on Electronic Systems

a. Licensees may store, process, or produce SGI on a stand-alone computer or computer network that is not connected to the Internet and that limits network access to SGI-authorized personnel only.

When a networked computer is used, it must not be physically or in any other way connected to a network that is accessible by users who do not have authorized access to SGI, in accordance with 10 CFR 73.22(g). Computers that are connected to the World Wide Web through the Internet or are connected to an Intranet that allows access to those that are not approved for access to SGI, are not considered stand-alone and must not be used to store, process, or produce SGI. Computers that are not located within an approved and lockable security storage container must have a removable hard drive with a bootable operating system that is used to load and initialize the computer as prescribed by 10 CFR 73.22(g)(2). SGI files must be encrypted on a stand-alone SGI computer prior to transmission over a computer that has network connectivity, as prescribed by 10 CFR 73.22(f)(3). (See Regulatory Positions C.7(a) through C.7(f) for additional guidance on SGI transmission procedures.) Licensees may produce, process, or store SGI-M on a computer or computer system, provided that the computer system is assigned to the licensee or

contractor's facility. In addition, the SGI-M files are to be protected by password or encryption as prescribed by 10 CFR 73.23(g)(1).

b. Licensees should not use Smart Phones or similar portable communication devices to process SGI and should only use laptop computers for that purpose if they have disabled the infrared port and network connectivity capability.

Licensees should properly configure portable laptops before processing SGI and ensure that users are aware of their responsibilities with respect to the safekeeping and storage of the portable laptops. Portable laptops used to process SGI must either be stored in a security storage container when not in use or have a removable hard drive with a bootable operating system, as prescribed by 10 CFR 73.22(g)(2) and 10 CFR 73.22(g)(3). Those removable hard drives, when not in use, must be marked to indicate that they contain SGI and be stored in a security storage container in accordance with 10 CFR 73.22(d)(4), 73.23(d)(4), 73.22(g)(3), and 73.23(g)(3). Licensees may use other mobile devices or systems if the NRC has approved their security in accordance with 10 CFR 73.22(g)(3) and 10 CFR 73.23(g)(3).

c. If a computer system containing sensitive unclassified information is to be sent out for service, the hard drive must be removed before the system leaves the facility to ensure that unauthorized personnel do not gain access to SGI, as prescribed by 10 CFR 73.22(b) and 10 CFR 73.23(b). The hard drive must be properly stored until the computer system is returned, in accordance with 10 CFR 73.22(c)(2) and 10 CFR 73.23(c)(2).

9. Removal from Safeguards Information Category

a. Documents or other matter originally containing SGI must be removed from the SGI category when the information no longer meets the criteria as defined by 10 CFR 73.2 and in accordance with 10 CFR 73.22(h) and 10 CFR 73.23(h).

b. Historical documents that are in storage need not be removed solely for the purpose of meeting the requirement of 10 CFR 73.22(h) and 10 CFR 73.23(h). As those documents are removed from storage for use (i.e., transmittal, modification, or use as an attachment), the documents' content should be examined to determine the applicability of the SGI designation. If, after review, a determination is made that the documents no longer meet the criteria for SGI designation, the documents must be removed from the SGI category, as prescribed by 10 CFR 73.22(h) and 10 CFR 73.23(h).

c. The authority to determine that a document or other matter may be decontrolled must be exercised only by the NRC, or with NRC approval, or in consultation with the individual or organization that made the original SGI determination, in accordance with 10 CFR 73.22(h) and 10 CFR 73.23(h).

d. Personnel should not remove the SGI designation from any document or material unless they themselves or their organization was responsible for the original SGI designation. All reasonable actions should be taken to inform known recipients of the SGI document or material that it has been removed from the SGI category. Licensees should use the following approach to decontrol documents and material:

(1) Draw a horizontal line through the SGI designation on the first page.

(2) Place initials adjacent to the horizontal line.

(3) Place the date, name, and title of the individual performing the SGI removal action adjacent to the horizontal line.

(4) Identify the new designation of the document or material, if applicable, directly beneath the original SGI designation.

(5) Draw a horizontal line through the SGI designation on each subsequent page of the document.

10. Destruction of Matter Containing Safeguards Information

a. Safeguards information must be destroyed when no longer needed or required to be maintained, as prescribed by 10 CFR 73.22(i) and 10 CFR 73.23(i).

Electronic media such as desktop workstations, laptops, notebook computers, and other devices often contain components for permanent program and data storage (e.g., the hard drive on a desktop workstation). When these components fail or are removed because they are no longer needed (surplus) or are obsolete, licensees should use specialized software or hardware to purge the media storage components (e.g., hard drive, memory card) of all residual data. Standard file deleting capabilities delete only the file reference, not the file itself. Reformatting a hard disk does not ensure that the stored data are unrecoverable. Destruction records are not required. To positively purge any residual data, the media storage device should be degaussed and, where applicable, destroyed.

b. Alternatively, a licensee-approved program should be used to completely overwrite the media multiple times with random patterns to an extent that information cannot be retrieved by means available to the general public. If neither of these options is available, the media should be destroyed. To reduce the risk of exposing sensitive information to disclosure or reproduction by unauthorized personnel, licensees should implement the following procedures when any media containing SGI are to be disposed of or transferred for nonexclusive use:

(1) Prohibitions on the destruction of media—Removable magnetic storage media, such as diskettes and tapes, containing SGI must not be disposed of in regular waste containers as prescribed by 10 CFR 73.22(i) and 10 CFR 73.23(i). .

(2) Burning and shredding of media—If degaussing is not possible, media should be destroyed by burning or with a crosscut shredder approved for the destruction of SGI.

(3) Destruction of defective media—Defective hard disk drives and removable storage media that contain SGI and that cannot be cleansed should be destroyed.

(4) Hard-disk media—If hard-disk drives are removed from or replaced in a workstation, the hard drive that is removed should have specialized software applied to purge the media contained therein. If this is not possible, hard disks should be degaussed and, where applicable, destroyed.

c. When the information is no longer needed, licensees must destroy documents or other nonelectronic matter containing SGI by burning, shredding, or any other method that precludes reconstruction by the public at large. Pieces no wider than 1/4 inch, composed of several pages

or documents and thoroughly mixed, are considered completely destroyed, as prescribed by 10 CFR 73.22(i) and 10 CFR 73.23(i). The pieces should not exceed 1/4 inch either vertically or horizontally. When a strip shredder is used as a means of destruction, care should be taken to ensure that pieces of the document are not larger than 1/4 inch and are thoroughly mixed with several other destroyed documents. The methods employed by commercial shredding companies are acceptable for the destruction of SGI documents, provided that a member of the licensee organization is present when the destruction occurs. Destruction methods that have been approved for classified information are also acceptable for the destruction of SGI.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[1] may use this regulatory guide, as well as the NRC's plans for using it. In addition, it describes the NRC staff's compliance with 10 CFR 50.109, "Backfitting," and any applicable finality provisions in 10 CFR Part 52.

This Regulatory Guide provides the NRC's first guidance on compliance with the Power Reactor Security Requirements rule (10 CFR Part 73, "Physical Protection of Plants and Materials," Section 73.22, "Protection of Safeguards Information,") published in the Federal Register on October 24, 2008 (73 FR 63546). As stated in the rule, the purpose of the rulemaking was, in part, to "implement generally applicable requirements for SGI that are similar to requirements imposed by the Orders. This rule became effective on February 23, 2009 (73 FR 63546, October 24, 2008). The statement of considerations (SOC) for the final Power Reactor Security Requirements rule discussed compliance with applicable backfitting provisions (73 FR 63565). The first issuance of guidance on a new rule does not constitute backfitting, inasmuch as the guidance must be consistent with the regulatory requirements in the new rule and the backfitting considerations applicable to the new rule must, as a matter of logic, also be applicable to this newly-issued guidance. Therefore issuance of this new Regulatory Guide does not constitute issuance of "new" guidance within the meaning of the definition of "backfitting" in 10 CFR 50.109(a)(1), nor does the issuance of this new Regulatory Guide, by itself, constitute an action inconsistent with any of the issue finality provisions in 10 CFR Part 52.

[1] In this section, "licensees" include applicants for standard design certifications under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

GLOSSARY

background check—At a minimum, includes a Federal Bureau of Investigation (FBI) criminal history records check (including verification of identity based on fingerprinting), employment history, education, and personal references. Title 10, Section 73.57, "Requirements for Criminal History Records Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information," of the *Code of Federal Regulations* (10 CFR 73.57) requires individuals engaged in activities subject to regulation by the U.S. Nuclear Regulatory Commission (the Commission or NRC), applicants for licenses to engage in Commission-regulated activities, and individuals who have notified the Commission in writing of an intent to file an application for licensing, certification, permitting, or approval of a product or activity subject to regulation by the Commission to conduct fingerprinting and criminal history records checks before granting access to Safeguards Information (SGI). A background check must be sufficient to support the trustworthiness and reliability determination so that the person performing the check and the Commission have assurance that granting an individual access to SGI does not constitute an unreasonable risk to the public health and safety or the common defense and security.

controlled access area—Any temporarily or permanently established area which is clearly demarcated, access to which is controlled and which affords isolation of the material or persons within it.

need to know—A determination by a person having responsibility for protecting SGI (including SGI designated as "Safeguards Information—Modified Handling," referred to as SGI-M) that a proposed recipient's access to SGI is necessary for the performance of official, contractual, licensee, applicant, or certificate holder employment. In an adjudication, "need to know" means a determination by the originator of the information that the information is necessary to enable the proposed recipient to proffer and/or adjudicate a specific contention in that proceeding, and the proposed recipient of the specific SGI possesses demonstrable knowledge, skill, training, or education to effectively utilize the specific SGI in the proceeding. Where the information is in the possession of the originator and the NRC staff (dual possession), whether in its original form or incorporated into another document or other matter by the recipient, the NRC staff makes the determination. In the event of a dispute regarding the "need-to-know" determination, the presiding officer of the proceeding shall make the "need to know" determination.

person—(1) Any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the U.S. Department of Energy (DOE) (except that DOE shall be considered a person to the extent that its facilities are subject to the licensing and related regulatory authority of the Commission pursuant to Section 202 of the Energy Reorganization Act of 1974 (Ref. 11) and Sections 104, 105, and 202 of the Uranium Mill Tailings Radiation Control Act of 1978 (Ref. 12)), any State or political subdivision of a State, or any political subdivision of any government or nation, or other entity, and (2) any legal successor, representative, agent, or agency of the foregoing.

protected area—An area encompassed by physical barriers and to which access is controlled.

reviewing official—An individual appointed by the licensee, and approved by the NRC, to independently make need-to-know determinations (for SGI in general) and review the results of licensee employee, applicant, and/or contractor background checks to make trustworthiness and reliability determinations as a condition for access to SGI. The reviewing official must be an individual with access to SGI or unescorted access and be in a position to determine other individuals' need to know through his or her official, contractual, or licensee duties.

Safeguards Information—Information not classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed control and accounting procedures for the physical protection of special nuclear material in quantities determined by the Commission through Order or regulation to be significant to the public health and safety or the common defense and security; detailed security measures (including security plans, procedures, and equipment) for the physical protection of source, byproduct, or special nuclear material in quantities determined by the Commission through Order or regulation to be significant to the public health and safety or the common defense and security; security measures for the physical protection of and location of certain plant equipment vital to the safety of production or utilization facilities; and any other information within the scope of Section 147 of the Atomic Energy Act of 1954, as amended, the unauthorized disclosure of which, as determined by the Commission through Order or regulation, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material.

Safeguards Information-Modified Handling—The designation or marking applied to SGI which the Commission has determined requires handling requirements modified from the specific SGI handling requirements that are applicable to SGI needing a higher level of protection.

security storage container—Includes any of the following repositories: (1) for storage in a building located within a protected or controlled access area, a steel filing cabinet equipped with a steel locking bar and a three-position, changeable combination, U.S. Government Services Administration (GSA) approved padlock, (2) a security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked "GSA-Approved Security Container" on the exterior of the top drawer or door, (3) a bank safety-deposit box, and (4) other repositories which, in the judgment of the NRC, would provide comparable physical protection.

trustworthiness and reliability—Characteristics of an individual considered dependable in judgment, character, and performance, such that disclosure of SGI (including SGI designated as "Safeguards Information—Modified Handling") to that individual does not constitute an unreasonable risk to the public health and safety or common defense and security. A determination of trustworthiness and reliability for this purpose is based upon a background check.

REFERENCES[2]

1. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

2. Atomic Energy Act of 1954, as amended.

3. EA-03-199, Order Imposing Requirements for Protection of Certain Safeguards Information, November 25, 2003.

4. Energy Policy Act of 2005 (EPAct) (Public Law No. 109 58, 119 Stat. 594.

5. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

6. Relief From Fingerprinting and Criminal History Records Check for Designated Categories of Individuals, Federal Register 71 FR 33989, June 13, 2006.

7. Protection of Safeguards Information, Federal Register 73 FR 63546, October 24, 2008.

8. 10 CFR 73.57, "Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information," U.S. Nuclear Regulatory Commission, Washington, DC.

09. NEI 03-01, "Nuclear Power Plant Access Authorization Program," dated April 2004.

10. Energy Reorganization Act of 1974, Public Law 93-438, October 11, 1974.

11. Uranium Mill Tailings Radiation Control Act of 1978, Public Law 95-604, November 8, 1978.

[2] Publicly available NRC published documents are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. The documents can also be viewed on-line or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail pdr.resource@nrc.gov.

REFERENCES[3]

1. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

2. Atomic Energy Act of 1954, as amended.

3. EA-03-199, Order Imposing Requirements for Protection of Certain Safeguards Information, November 25, 2003.

4. Energy Policy Act of 2005 (EPAct) (Public Law No. 109 58, 119 Stat. 594.

5. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

6. Relief From Fingerprinting and Criminal History Records Check for Designated Categories of Individuals, Federal Register 71 FR 33989, June 13, 2006.

7. Protection of Safeguards Information, Federal Register 73 FR 63546, October 24, 2008.

8. 10 CFR 73.57, "Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information," U.S. Nuclear Regulatory Commission, Washington, DC.

09. NEI 03-01, "Nuclear Power Plant Access Authorization Program," dated April 2004.

10. Energy Reorganization Act of 1974, Public Law 93-438, October 11, 1974.

11. Uranium Mill Tailings Radiation Control Act of 1978, Public Law 95-604, November 8, 1978.

[3] Publicly available NRC published documents are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. The documents can also be viewed on-line or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail pdr.resource@nrc.gov.