U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

July 2009
Division 5

DRAFT REGULATORY GUIDE

Contact: R. Norman
(301) 415-2278

DRAFT REGULATORY GUIDE DG-5034

(New Regulatory Guide)

PROTECTION OF SAFEGUARDS INFORMATION

A. INTRODUCTION

Title 10, Section 73.21, "Protection of Safeguards Information: Performance Requirements," of the *Code of Federal Regulations* (10 CFR 73.21) requires, in part, that each licensee, certificate holder, applicant, or other person who produces, receives, or acquires Safeguards Information (SGI) ensure that it is protected against unauthorized disclosure.

This guide describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable to implement the general performance requirements specified in 10 CFR 73.21(a)(i) and (ii) that establish, implement, and maintain an information protection system that includes the applicable measures for SGI specified in 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements," or 10 CFR 73.23, "Protection of Safeguards Information-Modified Handling: Specific Requirements." This guide applies to all licensees, certificate holders, applicants, or other persons who produce, receive, or acquire SGI (including SGI with the designation or marking: "Safeguards Information-Modified Handling" (SGI-M)).

The guidance and criteria contained in this document pertain to the protection of SGI as defined in 10 CFR Part 73, "Physical Protection of Plants and Materials." This document is intended to assist licensees and other persons who produce, receive, or acquire SGI to establish an information protection system that addresses (1) information to be protected, (2) conditions for access, (3) protection while in use

---

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received final staff review or approval and does not represent an official NRC final staff position.

Public comments are being solicited on this draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rulemaking, Directives, and Editing Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; e-mailed to nrcrep.resource@nrc.gov; submitted through the NRC's interactive rulemaking Web page at http://www.nrc.gov; or faxed to (301) 492-3446. Copies of comments received may be examined at the NRC's Public Document Room, 11555 Rockville Pike, Rockville, MD. Comments will be most helpful if received by October 1, 2009.

Electronic copies of this draft regulatory guide are available through the NRC's interactive rulemaking Web page (see above); the NRC's public Web site under Draft Regulatory Guides in the Regulatory Guides document collection of the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/doc-collections/; and the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML090930608.

or storage, (4) preparing and marking documents or other matter, (5) reproduction of matter containing SGI, (6) external transmission of documents and material, (7) processing SGI on electronic systems, (8) removal from the SGI category, and (9) destruction of matter containing SGI.

The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required.

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.

B. DISCUSSION

SGI is a special category of sensitive unclassified information to be protected from unauthorized disclosure under Section 147 of the Atomic Energy Act of 1954, as amended (AEA). 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 for the protection of SGI. Commission Orders issued since September 11, 2001, have also imposed requirements for the designation and 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" the information and an authorization based on an appropriate background check. Power reactors, certain research and test reactors, and independent spent fuel storage installations are examples of the categories of licensees currently subject to the provisions of 10 CFR Part 73 for the protection of SGI.

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. The Commission has, by Order, imposed SGI handling requirements on certain categories of these licensees. An example is the Order, EA 03-199, Order Imposing Requirements for Protection of Certain Safeguards Information, November 25, 2003, issued to certain materials licensees.

On February 11, 2005, the NRC published a proposed rule 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 for other SGI.

Subsequently, Congress enacted the Energy Policy Act of 2005 (EPAct) (Public Law No. 109-58, 119 Stat. 594). Section 652 of the EPAct amended Section 149 of the AEA to require the 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," 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.

The Commission exercised that authority to relieve by rule certain categories of persons from those requirements, including Federal, State, and local officials involved in security planning and incident response. 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. 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 this rulemaking. As part of the final SGI rulemaking, the commission made additional revisions to § 73.59 that 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). 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 that were not included in the final SGI rule that the NRC continues to view as an essential part of the NRC's SGI protection requirements.[1] 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 would have, at a minimum, resulted in further delay in 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 the Orders impose a more stringent requirement than the rule. The Commission will ultimately decide when and by what means it will relax the Orders and notify licensees accordingly.

[1] The NRC staff notes that the Commission has also expressed its concern with the continuing effectiveness of the reviewing official provision in that only last year, the Commission asked Congress for an amendment to Section 149 that would authorize the NRC to require fingerprinting of individuals responsible for making decisions regarding a person's trustworthiness and reliability. See letter to the Honorable Nancy Pelosi from Chairman Dale E. Klein, dated June 9, 2008 (Legislative Proposal Package, ADAMS Accession Number ML081550569).

The NRC staff also notes that, to the extent there may be a conflict between the Orders and the rule, the more stringent of the requirements would apply. For example, though the Orders only require 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 (that 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.

C. REGULATORY POSITION

1. 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).

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

   (a) document activities and commitments regarding the local procedures for the protection of information that are required by 10 CFR 73.22 (b) through (i) or 73.23(b) through (i),

   (b) identify key personnel with responsibilities for implementation,

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

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

   (e) establish a system for records review and retention,

   (f) establish procedures to address security violations, and

   (g) establish training programs and procedures regarding the identification and protection of SGI.

3. Any person, whether or not a licensee of the NRC, who produces, receives, or acquires SGI is subject to the requirements (and sanctions) of the SGI rule (hereafter referred to as the "rule").

   If information is considered SGI, but 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 a conservative manner and apply the protection provisions of 10 CFR 73.22(b) through (i), and obtain clarification from the originator as soon as practicable, so that the information can be protected at the appropriate level.

4. Licensees should inform Federal, State, and local law enforcement agencies of the SGI requirements before transferring SGI, so that these agencies are fully aware of the protection requirements for SGI and the potential for civil and criminal sanctions against any person that discloses SGI in an unauthorized manner.

   The conditions for transfer of SGI to a third party (e.g., need to know) would still apply to law enforcement agencies, as would sanctions for unlawful disclosure. Before sharing or providing third party access to SGI with an authorized recipient, it is the responsibility of the possessor to ensure that the SGI will be properly protected. For example, the possessor of SGI should have

written or oral confirmation that the recipient understands the protection and handling requirements prior to sharing the SGI.

These law enforcement agencies are presumed to meet the performance requirements of 10 CFR 73.21(a)(1) assuming that they do the following:

(a) implement controlled access areas and procedures for information use and storage,
(b) routinely use sensitive, unclassified information,
(c) adhere to sanitization and destruction principles,
(d) employ individuals who have been fingerprinted and have been the subject of a background check, and
(e) implement the need to know principle.

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

The Designation Guide for Safeguards Information, Criteria, and Guidance provides further examples of what information constitutes SGI and SGI-M. The guide is divided into two volumes to facilitate ease of use for individuals making SGI or SGI-M determinations. Regulations in 10 CFR 73.21 or in Commission Orders pertaining to security matters set forth criteria for determining whether a licensee's or applicant's information is SGI or SGI-M. Volume I of the designation guide describes information required to be designated SGI, such as security measures for power reactors and spent fuel. Volume II describes information required to be designated SGI-M, such as security measures for manufacturers and distributors of radioactive material and panoramic or underwater irradiators.

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 who 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 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 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 is information that discloses generic consequences to a class of facilities or material users. Normal engineering or construction drawings showing the location of safety-related equipment 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 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.

General information on local law enforcement armed responders, such as total complement and shift size, which is legitimately in the public domain, is not SGI and is not subject to protection under the rule or the AEA. Such information may be SGI when directly tied to the protection of, or in response to, a licensed facility.

6. Access to SGI requires that an individual have a need to know, be deemed trustworthy and reliable, and the subject of 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 upon verification of identity, employment history, education, criminal history records check, and appropriate reference checks as defined by "background check" in 10 CFR 73.2. The verification of a person's stated level of education 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. Licensees may use either personal references or developed references when collecting information to make a trustworthiness and reliability determination. 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.

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). The NRC expects licensees to use their best judgment and experience in determining which individuals are trustworthy and reliable and therefore suitable for access to SGI. The licensee should be judicious in his or her application of the trustworthiness and reliability standard. The adjudication standard should be capable of supporting a character determination.

The regulations contain no reinvestigation requirement for continuing access to SGI. However, the regulations at 10 CFR 73.22(b) and 73.23(b) require that persons with access to SGI be trustworthy and reliable, based on a background check. This implies that there is a continuing obligation for licensees and others responsible for allowing access to SGI to make reasonable efforts and use their best judgment to ensure that persons with access to SGI remain trustworthy and reliable.

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 73.23(b)(1). When relying upon 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 possesses such a clearance.

Persons possessing SGI access authorization at the time the final rule was published (October 24, 2008) need not undergo additional fingerprinting for continued access to SGI. To meet the requirements of the rule, employees that 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 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 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

If the employee has not been the subject of a trustworthiness and reliability determination, based upon a background check as prescribed in 10 CFR 73.22(b) and 73.23(b), he or she would have to undergo a background check before being granted or allowed continued access to SGI.

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 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, "Definitions."

7. The following individuals do not have to undergo fingerprinting and a criminal history records check per 10 CFR 73.59:

   (a) 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;

   (b) a Member of Congress;

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

   (d) 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;

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

   (f) 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;

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

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

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

   (j) 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

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

The individuals described above are considered trustworthy and reliable by virtue of their occupation, and they have either already undergone a background or criminal history check as a condition of their employment or are subject to direct oversight by government authorities in their day-to-day jobs.

Representatives of foreign governments, as described in 10 CFR 73.59(f), are not subject to fingerprinting and criminal history checks because those checks would not likely yield any information probative of the representative's trustworthiness and reliability - domestic criminal databases typically would not have records on foreign representatives. In addition, requiring fingerprinting and criminal history checks of foreign government representatives could strain existing cooperative relationships with the NRC's foreign counterparts, thus undermining the Commission's international efforts to enhance nuclear security. The rule does not require Commission approval for access to SGI by any foreign nationals, including representatives of foreign governments. However, representatives of foreign governments can only be exempt from the fingerprinting requirement of 73.59 with the approval of the Commission.

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 designated by a foreign government organization involved in nuclear emergency planning or incident response to serve as foreign government representatives before the NRC.

8. 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.

   Because Section 149 of the AEA currently only permits the NRC to collect fingerprints for persons seeking access to SGI or unescorted access to a designated facility, the designated reviewing official must be an individual seeking access to SGI or unescorted access to a designated facility and be in a position to determine other individuals' need to know for SGI as part of the individual's official duties.

9. Each licensee that is subject to the fingerprint provisions shall fingerprint each individual who requires access to SGI and submit the fingerprints to the NRC for transmission to the FBI in accordance with 10 CFR 73.22(b) and 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 making the trustworthiness and reliability determination. The NRC has accepted certain industry standards, such as those found in the Nuclear Energy Institute document, NEI 03-01, "Personal History Questionnaire," and considers them an acceptable means for licensees to use when making a trustworthiness and reliability determination.

10. 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). Licensees shall retain the documentation used to support or deny the trustworthiness and reliability determination 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 in accordance with 10 CFR 73.57(f)(5).

11. Each individual record of those requesting SGI access should contain documentation from the reviewing official that briefly explains the basis for granting or denying the request.

    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.

12. 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 on 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 and the physical characteristics of the individual.

13. 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 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.[2]

    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) and 73.23(c)(2). Security storage containers used to house SGI must not have exterior markings that identify the content of the matter contained within and

[2] Protection requirements differ significantly for information designated as SGI (10 CFR 73.22) and SGI-M (10 CFR 73.23). This section addresses acceptable means for both designations.

must preclude 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.

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 the following:

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

(b) 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

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

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

Under certain conditions, the general control exercised over protected or controlled access areas would be considered to meet this requirement. 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:

(a) the above-mentioned alarm stations, guard posts, and guard ready-rooms;
(b) an engineering or drafting area, if visitors are escorted;
(c) certain nuclear power plant vital areas, such as the control room or security office;
(d) plant maintenance areas, if access is restricted; or
(e) 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.

14. 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 the content of the matter contained within and must preclude 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.

15. Licensees should change the combination to the security storage container if compromise is suspected or individuals knowledgeable of the combination lose their need to know or access to SGI.

Each security storage container should have an associated record that is used to record its opening and closing. When security awareness inspections are conducted by fellow employees or guard force members, 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.

16. Licensees should conduct discussions involving 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.

17. 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 use encryption that is Federal Information Processing Standard (FIPS) 140-2, or later, compliant. 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.

18. Licensees may store, process, or produce SGI on a stand-alone computer or computer network that is not connected to the Internet, and 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 that 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 Section 15 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.

19. Licensees should not use a Smart-Phone or BlackBerry 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 laptops before processing SGI and ensure that users are aware of their responsibilities with respect to the safekeeping and storage of the laptops. 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)(3) and 73.22(g)(2). 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 their security is approved by the NRC in accordance with 10 CFR 73.2(g)(3) and 73.23(g)(3).

20. 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 due to the increased potential for inadvertent or unauthorized disclosure and the lack of adequate storage accommodations. In those instances when licensees grant authorization for SGI to be taken to one's 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, 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.

21. To indicate the presence of SGI, documents must be conspicuously marked at the top and bottom (preferably in 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) and 73.23(d)(1).

22. 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):

(a) the identification of the generating organization,
(b) the name and title of the SGI designating official,
(c) the date that the document or other matter was designated SGI, and
(d) an indication that unauthorized disclosure will be subject to civil and criminal penalties.

23. 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., transmitted, modified, or used 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).

To indicate that unauthorized disclosure is subject to civil and criminal penalties, as required by Sections 73.22(d)(1)(iii) and 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

When SGI has been removed from the security container, an SGI cover sheet 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.

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 73.23(d)(1).

24. Transmittal documents that do not contain SGI or any other sensitive information but have an SGI enclosure or attachment must be marked as a regular SGI document in accordance with 10 CFR 73.22(d)(3) and 73.23(d)(3).

In addition, the sentence, "When separated from Safeguards Information enclosure(s), this document is decontrolled," must be conspicuously placed at the bottom of the document. when the document contains no other sensitive information, as prescribed by 10 CFR 73.22(d)(2) and 73.23(d)(2). When SGI is included in transmittal documents that are forwarded to the NRC, portion markings should be used to distinguish those portions of the document that contain SGI as prescribed by 10 CFR 73.22(d)(3) and 73.23(d)(3). Every effort should be made to ensure that the transmittal document does not include SGI.

25. When impromptu and informal discussions or meetings occur, it is not necessary to turn off cell phones. 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 when discussing SGI. Taking such a proactive position, reduces the potential for an inadvertent transmission of SGI.

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

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

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

(c) ensure that no discussion takes place that is audible or visible to persons not authorized access to the information; and

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

First-line managers and above should be authorized to establish conferences involving SGI. Conferences may be held outside guarded or controlled areas only when security management is consulted for the purposes of obtaining appropriate guidance for the physical protection of SGI. Transcripts and meeting minutes or hearings that contain SGI must be marked and protected, in accordance with 10 CFR 73.22(d)(4) and 73.23(d)(4).

27. Licensees may reproduce SGI to the minimum extent necessary. 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 73.23(e). The evaluation should take into consideration the potential for retention of residual images on the copier.

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 73.23(e). Copiers that have been designated for the reproduction of SGI must be clearly identified. When reproducing SGI, paper jams should be cleared immediately and unwanted documents should be properly discarded.

28. 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 an authorized SGI user and has a need to know. Licensees should take the following steps when transmitting SGI:

(a) Hand-carry—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 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.

(b) Mail—When SGI is mailed, two sealed opaque envelopes or containers must be used.

(1). 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.

(2). 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 as prescribed by 10 CFR 73.22(f) and 73.23(f).

(3). 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 that which has been placed on the envelope or container.

(4). 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 73.23(f)(2). When express mail is used, a signature should be required.

(c) 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 the Federal Information Processing Standard (FIPS) 140-2, or later, encryption on a stand-alone computer processing unit as prescribed by 10 CFR 73.22(f)(3).

(d) 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.

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

(f) 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).

(g) 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 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.

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

The authority to determine that a document or other matter may be decontrolled must only be exercised by the NRC, 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 73.23(h).

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:

(a) Draw a horizontal line through the SGI designation on the first page.
(b) Place initials adjacent to the horizontal line.
(c) Place the date, name, and title of the individual performing the SGI removal action adjacent to the horizontal line.
(d) Identify the new designation of the document or material, if applicable, directly beneath the original SGI designation.
(e) Draw a horizontal line through the SGI designation on each subsequent page of the document.

If there is disagreement on the change of category, all differing opinions as to whether a

document should be removed from the SGI category should be referred to the NRC's Director, Division of Security Operations, Office of Nuclear Security and Incident Response, for final determination. Other disagreements regarding the removal of SGI from a category or a change in category should be referred to the office that generated the information.

30. Safeguard information must be destroyed when no longer needed or required to be maintained as prescribed by 10 CFR 73.22(i) and 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 purge the media storage components (e.g., hard drive, memory card) of all residual data, using specialized software or hardware. Standard file deleting capabilities only delete the file reference, not the file itself. Reformatting a hard disk does not ensure that the stored data is unrecoverable. Destruction records are not required. To positively purge any residual data, the media storage device should be degaussed and where applicable, destroyed.

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:

(a) 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.

(b) 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.

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

(d) Hard-disk media—If hard-disk drives are removed from or replaced in a workstation, the hard drive that is removed should be unconditionally formatted before removal. If this is not possible, hard disks should be degaussed before destruction.

(e) Media maintenance—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 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 73.23(c)(2).

When the information is no longer needed, licensees must destroy documents or other non-electronic 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 73.23(i). When measured vertically and horizontally, the pieces should not exceed 1/4 inch. 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 to licensee, certificate holders, applicants, or other persons who produce, receives, or acquires Safeguards Information regarding the NRC's plans for using this regulatory guide. The NRC does not intend or approve any imposition or backfit in connection with its issuance.

In some cases, applicants or licensees may propose or use a previously established acceptable alternative method for complying with specified portions of the NRC's regulations. Otherwise, the methods described in this guide will be used in evaluating compliance with the applicable regulations for license applications, license amendment applications, and amendment requests.

The NRC has issued this draft regulatory guide to provide additional guidance on implementation of and compliance with the SGI protection regulations, and to encourage public participation in its development. In some cases, licensees and other persons may propose methods for complying with specified portions of the NRC's regulations other than those described in this regulatory guide. This is acceptable, as long as such measures meet the requirements of the regulations. However, in the absence of any other acceptable method, the NRC staff intends to use the methods described in this regulatory guide as a baseline in evaluating compliance with the applicable regulations. The NRC will consider all public comments received in development of the final guidance document.

REGULATORY ANALYSIS

Statement of the Problem

Full compliance with the NRC's regulations for the protection of SGI is required as of February 23, 2009. The regulations require protection of SGI for a larger number of licensees and other entities than under the previous regulations. Additionally, the previously published guidance document (NUREG-0794, "Protection of Unclassified Safeguards Information," issued October 1981) is no longer considered appropriate for use, as the regulatory requirements have changed, and technology has advanced to the point of requiring new strategies. This regulatory guide should be used as a primary reference for implementation guidance on the existing regulation for the protection of safeguards information.

Therefore, issuance of this regulatory guidance is necessary to provide regulated entities or other groups that may handle, possess, or disseminate SGI with appropriate methods to meet the regulatory requirements of 10 CFR 73.21, 73.22, and 73.23.

Objective

The objective of this regulatory guide is to provide a means to assist licensees and other persons who possess SGI in establishing an information protection system that satisfies the requirements of 10 CFR 73.21, 73.22, and 73.23.

Alternative Approaches

The NRC staff considered the following alternative approaches:

Do not revise NUREG-0794.
Issue a new regulatory guide.

Alternative 1: Do Not Revise NUREG-0794

Under this alternative, the NRC would not issue additional guidance, and the guidance in NUREG-0794 would be retained. If the NRC does not take action, there would not be any changes in costs or benefit to the public, licensees, or the NRC. However, the "no-action" alternative would not address identified concerns with the current NRC guidance. This alternative provides a baseline condition from which any other alternatives will be assessed.

Alternative 2: Issue a New Regulatory Guide

Under this alternative, the NRC would issue a new regulatory guide, taking into consideration the lessons learned from industry and guidance that has already been issued on the subject. One benefit of this action is that it would enhance understanding among the groups that handle SGI, as well as others who might handle SGI in certain situations (e.g., hearings).

The impact to the NRC would be the costs associated with preparing and issuing the regulatory guide. The impact to the public would be the voluntary costs associated with reviewing and providing comments to the NRC during the public comment period. The value to the NRC staff and its applicants would be the benefits associated with enhanced efficiency and effectiveness in using a common guidance document as the technical basis for license applications and other interactions between the NRC and its regulated entities.

Conclusion

Based on this regulatory analysis, the NRC staff recommends issuance of a new regulatory guide. The staff concludes that the proposed action will enhance understanding of the SGI requirements and increase information sharing among authorized parties, consistent with direction from the Executive Branch. It could also lead to cost savings for the industry, especially with regard to encouraging consistency of plans and procedures to handle SGI by reducing the inefficiencies of duplication or improper implementation.

Backfit Analysis

The Commission has concluded, on the basis of the documented evaluation in the regulatory analysis, that none of the guidance in this regulatory guide are backfits as defined in 10 CFR 50.109(a)(4)(ii), 70.76(a)(4)(iii), 72.62 and 76.76(a)(4)(ii). The Commission has also concluded that the guidance in this regulatory guide is necessary to ensure that the facilities and materials described in the regulatory guide provide adequate protection to the public health and safety and are in accord with the common defense and security as applicable. Therefore, a backfit analysis is not required and the cost-benefit standards of 10 CFR 50.109(a)(3), 70.76, 72.62, and 76.76, do not apply. The documented evaluation in the regulatory analysis includes a statement of the objectives of and the reasons for the backfits that will be required by the regulatory guide and sets forth the Commission's conclusion that these backfits are not subject to the cost benefit standards of 10 CFR 50.109(a)(3), 70.76, 72.62, and 76.76.

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 (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 are assured that granting an individual access to SGI would not constitute an unreasonable risk to public health and safety or the common defense and security.

Need to know—A determination by a person having responsibility for protecting SGI (including SGI designated as "Safeguards Information-Modified Handling") that a proposed recipient's access to SGI is necessary in the performance of the duties of an official, contractor, licensee, applicant, or certificate holder. 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 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 use 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 should 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 and Sections 104, 105, and 202 of the Uranium Mill Tailings Radiation Control Act of 1978), 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.

Reviewing official—An individual appointed to independently review the results of a background check and make the determinations that the individual is trustworthy and reliable and has a valid need to know the SGI. The reviewing official should be an individual with access to SGI and have meet the same threshold for background checks and be in a position to determine the other individual's need to know through his or her official, contractual, or licensee duties.

Safeguards Information—Information not classified as National Security Information or Restricted Data that 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 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 that the Commission has determined requires modified handling requirements, because of the lower risk posed by the unauthorized disclosure of the information.

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 padlock approved by the U.S. Government Services Administration (GSA); (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 that, 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 public health and safety or common defense and security. A determination of trustworthiness and reliability for this purpose is based on a background check.

REFERENCES[3]

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

2. NUREG-0794, "Protection of Unclassified Safeguards Information," October 1981.

3. RIS 2002-15, "NRC Approval of Commercial Data Encryption Products for the Electronic Transmission of Safeguards Information," Revision 1, January 26, 2006.

4. DG-SGI-1, "Designation Guide for Safeguards Information, Criteria and Guidance," September 2005.

5. Atomic Energy Act of 1954, as amended, Sections 147 and 149.

[3] Publicly available NRC published documents such as Regulations, Regulatory Guides, NUREGs, and Generic Letters listed herein are available electronically through the Electronic Reading Room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. Copies are also available for inspection or copying for a fee from 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.