UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NEW REACTORS
OFFICE OF NUCLEAR REACTOR REGULATION
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS
OFFICE OF FEDERAL AND STATE MATERIALS AND
ENVIRONMENTAL MANAGEMENT PROGRAMS
WASHINGTON, DC 20555-0001

DATE

NRC REGULATORY ISSUE SUMMARY 2009-XX IMPLEMENTATION OF NEW FINAL RULE, PROTECTION OF SAFEGUARDS INFORMATION

ADDRESSEES

Each NRC licensee, certificate holder, applicant, or other person who produces, receives, or acquires Safeguards Information, including Safeguards Information (SGI) with the designation or marking Safeguards Information-Modified Handling (SGI-M), including but not limited to:

(1) All holders of licenses, including those undergoing decommissioning, for nuclear power reactors under the provisions of Title 10 of the Code of Federal Regulations (10 CFR) Part 50, “Domestic Licensing of Production and Utilization Facilities.”

(2) All holders of licenses, including those undergoing decommissioning, for research and test reactors.

(3) All holders of licenses, including those undergoing decommissioning, for Category I fuel cycle facilities; Category III fuel cycle facilities; enrichment facilities; and conversion facilities.

(4) Certain licensees authorized to manufacture and distribute items containing radioactive material.

(5) Certain panoramic and underwater irradiator licensees authorized to possess greater than 10,000 curies.

(6) All current and potential applicants for an early site permit (ESP), limited work authorization (LWA), standard design certification (DC), or combined license (COL) for construction and operation of nuclear power plants under the provisions of 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.”

(7) All Radiation Control Program Directors and State Liaison Officers.

(8) Licensees who transport radioactive materials quantities of concern.

ML090420054

PURPOSE

The U.S. Nuclear Regulatory Commission (NRC, the Commission) is issuing this regulatory issue summary (RIS) to remind all stakeholders of the significant changes to Title 10 of the *Code of Federal Regulations* (10 CFR) Parts 73.21, 73.22 and 73.23. This RIS provides clarifying information of the impact of the new rule [rule] (effective date February 23, 2009). This RIS requires no action or written response on the part of an addressee.

BACKGROUND INFORMATION

Previously, many licensees, applicants, certificate holders, or other persons were issued NRC Orders [orders] in the aftermath of the terrorist attacks of September 11, 2001, that required them to protect certain detailed information designated as SGI or SGI-M. Further orders were issued after the enactment of the Energy Policy Act of 2005 (EPAct), which expanded the NRC's fingerprinting authority with respect to access to SGI.

SGI, which includes both SGI and SGI-M, is a special category of sensitive unclassified information that licensees must protect from unauthorized disclosure under Section 147 of the Atomic Energy Act of 1954 (AEA), as amended. Section 147 of the AEA gives the Commission authority to designate, by regulation or order, other types of information as SGI. For example, Section 147.a.(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 that the Commission determines to be significant to the public health and safety or the common defense and security. Prior to the events of September 11, the Commission implemented its Section 147 authority through regulations in 10 CFR Part 73, sections 21 and 57. These requirements generally applied to security information associated with nuclear power plants, formula quantities of strategic special nuclear materials, and the transportation of irradiated fuel.

However, changes in the threat environment after September 11, 2001, have resulted in the need to protect additional types of security-related information held by a broader group of persons, including licensees, applicants, vendors, and certificate holders as SGI. Subsequently, the NRC issued orders that increased the number of licensees whose security measures would be protected as SGI and added various types of security-related information that would be considered SGI. For example, EA-04-190 was issued to certain NRC byproduct materials licensees on November 4, 2004 (69 Federal Register (FR) 65470, November 12, 2004). The Commission determined that the unauthorized release of this information could harm the public health and safety and the Nation's common defense and security, and damage the Nation's critical infrastructure, including nuclear power plants and other facilities and materials licensed and regulated by the NRC or Agreement States.

Subsequently, Congress enacted the EPAct (Public Law No. 109–58, 119 Stat. 594). Section 652 of the EPAct amended Section 149 of the AEA to require the fingerprinting of a broader class of persons for the purpose of checking criminal history records. Prior to the enactment of 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 the fingerprint identification and criminal history records check along with other elements of the background check requirement. Categories of individuals relieved from the background check are described in 10 CFR § 73.59.

In addition to the orders described earlier, the NRC issued more orders to licensees to impose the fingerprinting requirements mandated by the EPAct. Those orders were issued to the same persons who had previously received SGI protection orders, and required fingerprinting for an FBI identification and criminal history record check for any person with access to SGI. One significant aspect of the SGI fingerprinting orders was the requirement that the recipients designate a "reviewing official" who needed access to SGI, and who would be required to be approved by the NRC as "trustworthy and reliable" based on the NRC's review of his or her fingerprint-based criminal history records (e.g. Order EA-06-155; 71 FR 51861, 51862, August 31, 2006, Paragraph C.2). The orders specified that only the NRC-approved reviewing official could make determinations of access to SGI for the licensee. In addition, the SGI fingerprinting orders did not require the fingerprinting of a licensee employee who "…has a favorably-decided U.S. Government criminal history check within the last five (5) years, or has an active federal security clearance" *id*. (Paragraph A.3).

All of the orders issued by the NRC contained a relaxation clause that generally permitted the order issuing official (NRC Office Director) to "in writing, relax or rescind any of the above conditions upon demonstration of good cause by the Licensee." The cumulative efforts of the staff to increase the protection requirements associated with SGI and SGI-M, culminated in a final rulemaking. 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."

DISCUSSION

Since publication of the rule on October 24, 2008, licensees and other stakeholders who routinely use SGI have raised a number of questions with the NRC staff regarding guidance for the rule, which was implemented on February 23, 2009. All persons subject to the rule's requirements (meaning any person, including licensees, vendors, industry groups, etc. who are currently in possession of SGI) were required to be in compliance with the rule by the implementation date. Based upon stakeholder questions and comments concerning implementation of the rule, the NRC is issuing this RIS to review rule requirements and articulate the NRC staff's position on several implementation issues. Stakeholders are advised to closely examine the rule itself to ensure that they are in compliance with all requirements.

- Continuing Effect of the Orders

  A frequently asked question from stakeholders has been whether the rule supersedes the existing orders. The NRC staff is currently examining this issue, as well as the need for additional SGI rulemaking. As noted earlier, the orders contain several provisions that were not included in the rule, such as the requirement for a "reviewing official," that the NRC staff continues to view as an essential part of the NRC's SGI protection

requirements.[1] However, throughout the course of the rulemaking process, the NRC issued additional Orders to licensees and stakeholders governing the protection and handling of SGI. Those additional Orders included several requirements which were not included in the new rule. Incorporating those additional requirements into the new SGI rule would have required that the rule be re-noticed and published in the *Federal Register*. The limited number of licensees that received additional Orders, containing additional requirements that were not included in the rule, are implementing coordinated information security requirements that are under consideration for implementation by a larger segment of the licensee population. Orders containing requirements that were not published in the rule or are otherwise more stringent than the rule, will remain in effect until the Commission relaxes the requirements of the Orders in whole or in part. 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 have to decide when and by what means it will relax the orders.

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, the background check requirements of the rule would be imposed as a prerequisite for access to SGI. Additionally, order recipients would still be obligated to maintain an NRC-approved reviewing official, as required by the order.

- Grandfathering of Persons with Current Access to SGI

  Several licensees have asked if the access requirements set forth in the rule are applicable to all current and future persons subject to the rule's requirements. Persons who have not been subjected to the rule's background check requirement (i.e. the employment history, education history and personal references check), must complete such checks and be found to be trustworthy and reliable by the reviewing official or responsible party before they are permitted access to any SGI. This does not mean that individuals who have recently been subject to an equivalent background check (such as for unescorted access or for access to national security information), will have to re-accomplish a background check simply for access to SGI. The rule requirements are intended to apply to those individuals to whom these requirements have not been applied or have not otherwise been applied in a reasonably recent time period.

- Expanded Applicability of the Rule

  An important change to SGI requirements reflected in the rule is the expansion of the applicability to all persons who use SGI. Based upon the requirements of the previous version of the rule, section 73.21(a), the only person subject to the SGI protection requirements by regulations were licensees who possessed formula quantities of strategic special nuclear material, who were authorized to operate a nuclear power reactor, who transported a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel, or to persons who dealt with SGI through a

[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).

relationship with any of these categories of licensees. Pursuant to the rule, 10 CFR 73.21(a)(1), the previously mentioned limitation has been eliminated, such that the rule applies broadly to "Each licensee, certificate holder, applicant or other person who produces, receives, or acquires Safeguards Information (including Safeguards Information with the designation or marking: Safeguards Information-Modified Handling) shall ensure that it is protected against unauthorized disclosure."

- Elimination of Categories of Persons Permitted Access to SGI

  Under the previous SGI rule, only categories of persons specifically identified in paragraphs 73.21(c)(1)(i) through (vi), or specifically approved by the Commission on a case by case basis, were permitted access to Safeguards Information. This often resulted in a lengthy approval process when certain persons sought access to SGI who were not included within one of the listed categories. The rule no longer contains this restriction. Therefore, any person who has a need to know and who has been determined by the possessor of the SGI to be trustworthy and reliable, based on meeting all elements of a background check, may have access to SGI.

- Validity of Active Federal Security Clearances

  Several licensees have asked the NRC whether personnel with active Federal security clearances (e.g. "Q" or "L" clearances) would be required to have additional fingerprinting and background checks for purposes of having access to SGI. These stakeholders noted that, although the orders essentially relieved these individuals from being fingerprinted for access to SGI (e.g. Order EA-06-155; 71 FR 51861, 51862, August 31, 2006, Paragraph A.3), the rule does not contain provisions for continuing this practice.

  It is the NRC staff's determination that the rule does not require additional fingerprinting and background checks for persons with active Federal security clearances, provided that sufficient documentation of the active security clearance can be obtained by the reviewing official or responsible party. Rather than being "relieved" from the fingerprinting and background check requirement, such individuals are considered to have satisfied the requirements through other means, namely, the completion of their national security clearance investigations. This reflects a long-standing practice of the Commission as reflected in the hundreds of SGI fingerprinting orders that it has issued.

- Relief From Fingerprinting

  In response to licensee questions of "relief from fingerprinting" requirements, the NRC staff provides the following clarification. As noted in the previous section, persons with active Federal security clearances are not "relieved" from being fingerprinted, but rather may continue to have access to SGI based on the fingerprinting for their national security clearance investigation and their meeting all other access requirements. However, 10 CFR 73.59 does identify categories of persons assigned or occupying certain positions that are categorically relieved from fingerprinting by virtue of their occupational status. These categories of personnel were originally published in an Immediately Effective Final Rulemaking that created 10 CFR 73.59 (71 FR 33989, June 13, 2006). The rule maintains the majority of those relief provisions, with several modifications and additions. One notable benefit is, 10 CFR 73.59 relieves from fingerprinting "any agent, contractor, or consultant of the aforementioned persons who

has undergone equivalent criminal history records checks to those required by 10 CFR 73.22(b) or 10 CFR 73.23(b)."

It is also important to note that personnel relieved from fingerprinting and other elements of the background check requirement by 10 CFR 73.59 are still required to possess a valid need to know prior to obtaining access to SGI or SGI-M.

- Storage of SGI or SGI-M

  Some licensees raised questions concerning the storage of SGI. The section that addresses the protection of SGI while in use and storage was modified by the rule, sections 73.22(c)(1) and 73.23(c)(1), to recognize that SGI can be considered "under the control of an individual authorized access to SGI" when it is attended by such a person though not constantly being used. Safeguards Information within alarm stations, or rooms continuously occupied by authorized individuals need not be stored in a locked security container. As has always been the case, SGI must be stored in a locked security storage container when unattended. In contrast, SGI controlled as SGI-M need only be stored in a locked file drawer or cabinet. In either case, the rule requires that the container where SGI or SGI-M is stored shall not bear markings that identify the contents.

- Marking, Reproduction, and Transmittal of SGI or SGI-M

  Marking Requirements:
  In response to questions concerning the marking, reproduction and transmittal of Safeguards Information, the NRC staff provided responses, as summarized here. The SGI document marking requirements were changed to assist the reader with the identification of the document's designator and the date that the document or material was designated as SGI. The first page of SGI documents or other matter must now contain the name, title, and organization of the individual authorized to make a SGI determination and who has determined that the document or other matter contains SGI. The document or other matter must also identify the date that the determination was made, and indicate that unauthorized disclosure will be subject to civil and criminal sanctions. Additional instructions were provided to aid those tasked with creating transmittal letters or memoranda to the NRC that do not in themselves contain SGI, but are associated with attachments or enclosures that do.

  Transmittal Letters:
  When transmittal letters or memoranda to the NRC include enclosures that contain SGI but do not themselves contain SGI or any other form of sensitive unclassified information, the transmittal letter or memorandum shall be conspicuously marked on the top and bottom with the words "Safeguards Information." In addition to the SGI marking at the top and bottom of the transmittal letter or memorandum, the bottom of the transmittal letter or memorandum shall be marked with text to inform the reader that the document is decontrolled when separated from SGI enclosure(s).

  Correspondence to the NRC:
  Correspondence to the NRC containing SGI and non-SGI must be portion marked (i.e., cover letters, but not the attachments) to allow the recipient to identify and distinguish those sections of the correspondence or transmittal document containing SGI from those that do not. The portion marking requirement is no longer applicable to facility guard

qualification and training plans. The new rule has also removed the guidance that allowed documents and other matter containing SGI in the hands of contractors and agents of licensees that were produced more than one year prior to the effective date of the old rule to go unmarked as SGI documents, as long as they remained in storage containers and were not removed for use. Those documents and other matter, whether or not removed from storage containers for use, must now be properly marked as SGI documents.

It is important to note, however, that the rule does not require current possessors of SGI to retroactively mark SGI documents that were produced prior to the effective date of the rule. As noted by the Commission in the rule, "the Commission does not expect that licensees or applicants must go back and mark documents for which a cover sheet was used for the required information instead of the first page of the document, as set forth in 10 CFR 73.22(d)(1)" (73 FR 63557).

Safeguards Information may continue to be reproduced to the minimum extent necessary, consistent with need without permission of the originator. Equipment used to reproduce SGI must be evaluated to ensure that unauthorized individuals cannot obtain SGI by gaining access to retained memory or through network connectivity.

Packaging Requirements:
The rule is more explicit concerning the packaging requirement for SGI that is transmitted outside an authorized place of use or storage. Sections 73.22(f) and 73.23(f) of the rule, now state that SGI or SGI-M, when transmitted outside an authorized place of use or storage, must be packaged in two sealed envelopes or wrappers to preclude disclosure of the presence of protected information. The inner envelope or wrapper must contain the name and address of the intended recipient and be marked on both sides, top and bottom, with the words “Safeguards Information” or “Safeguards Information-Modified Handling,” as applicable. The outer envelope or wrapper must be opaque, addressed to the intended recipient, must contain the address of the sender, and shall not bear any markings or indication that the document or other matter contains SGI or SGI-M. Properly packaged SGI, when transported, must be transported by a means authorized by 10 CFR 73.22(f) and 73.23(f).

The new rule no longer makes reference to the use of “messenger-couriers” for the transportation of SGI. It now allows SGI and SGI-M to be transported by any commercial delivery company that provides service with computer tracking features. It also authorizes the continued use of U.S. first class, registered, express, or certified mail for the transportation of SGI. Individuals authorized to access SGI or SGI-M may also transport SGI or SGI-M outside of an authorized place of use or storage.

Electronic Transmission:
The NRC continues to allow for exceptions when SGI is transmitted under emergency or extraordinary conditions. Additionally, a requirement was added to change what was stated as “protected telecommunications circuits approved by the NRC” to “NRC approved secure electronic devices, such as facsimiles or telephone devices.” The authorized use of those NRC-approved devices is conditional and based upon the transmitter’s and receiver’s compliance with information security prerequisites. To meet the requirements, the transmitter and receiver must implement processes that will provide high assurance that SGI is protected before and after the transmission. Electronic mail, transmitted through the internet, is permitted provided that the

information is encrypted by a method (Federal Information Processing Standard [FIPS] 140-2 or later) approved by the appropriate NRC office. The information must be produced on a self-contained secure automatic data process system. Transmitters and receivers must implement information handling processes that will provide high assurance that SGI is protected before and after transmission.

- Electronic Processing of SGI or SGI-M

  The requirements for processing SGI on automatic data processing systems have not been significantly revised by the new SGI rule. However, there are noticeable differences between the requirements for processing SGI and SGI-M on computers. For SGI, automatic data processing systems used to process or produce SGI must continue to be isolated, such that they cannot be connected to a network accessible by users who are not authorized to access SGI. The requirement that an entry code be used to access the stored information has been deleted. Each computer used to process SGI that is not located within an approved and lockable security storage container must have a removable storage medium with a bootable operating system. The bootable operating system must be used to load and initialize the computer. The removable storage medium must also contain the software application programs and be secured in a locked security storage container when not in use.

  A mobile device such as a laptop may be used for processing SGI, provided that the device is secured in a locked security storage container when not in use. Where previously not addressed in the old rule, the new rule makes an allowance for electronic systems that have been used for storage, processing, or production of SGI to migrate to non-SGI exclusive use. Any electronic system that has been used for storage, processing, or production of SGI must be free of recoverable SGI prior to being returned to nonexclusive use.

  However, SGI-M need not be processed on a stand-alone computer. The rule permits SGI-M to be stored, processed, or produced on a computer or computer system, provided that the system is assigned to the licensee's or contractor's facility. SGI-M files must be protected, either by a password or encryption. Word processors such as electronic typewriters are not subject to these requirements as long as they do not transmit information off-site.

- Removal from SGI or SGI-M Category

  When documents or other matter are removed from the SGI category because the information no longer meets the criteria, care must be exercised to ensure that any document or other matter decontrolled not disclose SGI in some other form or be combined with other unprotected information to disclose SGI. The authority to determine that a document or other matter may be decontrolled will only be exercised by the NRC, with the NRC approval, or in consultation with the individual or organization that made the original SGI determination.

- Destruction of Matter Containing SGI or SGI-M

  The rule now states that SGI and SGI-M shall be destroyed when no longer needed. The information can be destroyed by burning, shredding, or any other method that precludes reconstruction by means available to the public at large. Of particular note,

the new rule considers documents destroyed when piece sizes no wider than one quarter inch composed of several pages or documents are thoroughly mixed.

The NRC will continue to evaluate its requirements, policies and guidance concerning the protection and unauthorized disclosure of SGI. Licensees, certificate holders, applicants and other persons who produce, receive, or acquire SGI will be informed of proposed revisions or clarifications.

BACKFIT DISCUSSION

This RIS does not represent a new or different staff position regarding the implementation of 10 CFR 73.21, 10 CFR 73.22 or 10 CFR 73.23. It requires no action or written response. Any action by addressees to implement changes to their safeguards information protection system, or procedures in accordance with the information in this RIS ensures compliance with 10 CFR Part 73 and existing orders, is strictly voluntary and therefore, is not a backfit under 10 CFR 50.109, "Backfitting." Consequently, the NRC staff did not perform a backfit analysis.

FEDERAL REGISTER NOTIFICATION

A notice of opportunity for public comment on this RIS was published in the Federal Register 74FR10786 on March 12, 2009 for a 30-day comment period. Five organizations provided comments to the RIS and those comments, as well as the NRC response to those comments, can be viewed in the Agencywide Document Access and Management System (ADAMS) under accession number ML091550003. The comments were considered and the RIS was updated accordingly.

CONGRESSIONAL REVIEW ACT

The NRC has determined that this RIS is not a rule under the Congressional Review Act (5 U.S.C. §§ 801–808) and, therefore, is not subject to the Act.

PAPERWORK REDUCTION ACT STATEMENT

This RIS does not contain new or amended information collection requirements subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). Existing information collection requirements were approved by the Office of Management and Budge, control number 3150-0002.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid Office of Management and Budget control number.

CONTACT (For Final Version of RIS)

Please direct any questions about this matter to the technical contact listed below.

Timothy J. McGinty, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Technical Contact: Robert Norman, NSIR/DSO
301-415-2278
E-mail: robert.norman@nrc.gov

CONTACT

Please direct any questions about this matter to the technical contact listed below.

Timothy J. McGinty, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Technical Contact: Robert Norman, NSIR/DSO
301-415-2278
E-mail: robert.norman@nrc.gov

DISTRIBUTION:
NSIR Reading File
PGCB Reading File

ADAMS ACCESSION NO.: ML090420054

OFFICE	ISB/DSO/NSIR	QTE	C:ISB/DSO/NSIR	C:RSOB/DSO/NSIR
NAME	RNorman		ALSilvious	RWay
DATE	6/3/09	2/4/09	6/3/09	6/4/09
OFFICE	D:DSO/NSIR	OD:OE	D:DORL/NRR	OGC:
NAME	PHolahan	DFurst	JGiitter	
DATE	6/16/09	03/14 /09	05/25/09	07/ /09
OFFICE	OGC:CRA	D:FCSS/NMSS	D:DWMEP/FSME	D:DNRL/NRR
NAME	Through JZorn	DDorman	LCamper	DMatthews
DATE	03/02/09	07/ /09	06/12/09	03/24/09
OFFICE	OD: OIS	PGCB/DPR/LA	PGCB/DRP/NRR	DMSSA/FSME
NAME	DTremaine	CHawes	SStuchell	RLewis
DATE	06/30/2009	06/ /09	06/ /09	06/12 /09
OFFICE	BC:PGCB/NRR	D:DPR/NRR		
NAME	MMurphy	TMcGinty		
DATE	06/ /09	06/ /09		

OFFICE RECORD COPY