

UNCLASSIFIED

**U.S. NUCLEAR REGULATORY COMMISSION INVENTORY OF
PROCEDURES GOVERNING SENSITIVE BUT UNCLASSIFIED OR
EQUIVALENT CONTROLLED UNCLASSIFIED INFORMATION**

MARCH 16, 2006

Section 1. General Questions

This section contains a series of questions that will normally apply to all categories of SBU or equivalent CUI used by your department or agency. In your responses, please note any differences in procedures between specific categories of information.

Are there any special policies or procedures for marking, handling, or accessing information covered by more than one category of SBU information or that is classified per Executive Order 12958 but may also fall into one or more SBU or equivalent CUI categories?

Yes. At the NRC there are two categories of SBU: Safeguards Information (SGI) and Sensitive Unclassified Non-Safeguards Information (SUNSI). SGI is information related to certain nuclear facility equipment or significant quantities of radioactive materials and the protection of such equipment and materials from malevolent threats such as the terrorist actions of September 11, 2001. Criteria for handling, marking and accessing SGI for NRC licensees are contained in 10 CFR 73.21, "Requirements for the protection of Safeguards Information." Additionally, Orders issued by the NRC Commission subsequent to the September 11, 2001 terrorist acts describe additional security measures designated as SGI in accordance with the authority granted under section 147 of the Atomic Energy Act of 1954, as amended (AEA). In some cases, these Orders contain special protection requirements for the information contained in and covered by the Orders. NRC Management Directive and Handbook 12.6, "NRC Sensitive Unclassified Information Security Program," describes who within NRC is authorized to designate information as SGI and how to protect it. The information remains designated as SGI until it no longer meets the criteria outlined in 10 CFR 73.21(b) or Commission Orders consistent with the authorization granted to the NRC by the AEA. After September 11, 2001, the NRC staff reviewed NRC policies and consolidated 23 types of sensitive unclassified non-safeguards information into the current SUNSI groups based on similar handling, marking and protection criteria. Two categories of SUNSI information that pertain to SBU involve allegation information and security related information. SUNSI means any unclassified non-safeguards information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal programs, or the personal privacy of individuals. On October 26, 2005, the NRC posted "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" to the NRC internal SUNSI Web site. The policy is also electronically available in the Agency-wide Documents Access and Management System (ADAMS). The Commission is currently reviewing the current SUNSI policy for possible revision.

Is there any consolidated departmental or agency registry of SBU markings?

Yes. SGI markings for the NRC are contained in NRC Management Directive and Handbook 12.6, "NRC Sensitive Unclassified Information Security Program." In addition, some of the Orders issued by the NRC Commission to certain classes of its

UNCLASSIFIED

UNCLASSIFIED

	<p>licensees contain special SGI marking requirements and examples. In order to distinguish information needing modified protection requirements from the SGI for reactors and fuel cycle facilities that require a higher level of protection, some Commission Orders have used the term "Safeguards Information-Modified Handling" (SGI-M) as the distinguishing marking for certain materials licensees. Lastly, the NRC is currently amending 10 CFR Part 73 to include SGI and SGI-M marking examples. Markings for the individual SUNSI groups are consolidated in "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information." The individual SUNSI group markings are also specified in the NRC internal SUNSI Web site.</p>
Does your department or agency provide any guidance to other agencies for handling SBU information originated in your agency?	<p>Yes. In addition to the requirements of 10 CFR Part 73, the NRC has issued NUREG-0794, "Protection of Unclassified Safeguards Information," as a guide to assist NRC licensees and other stakeholders who possess SGI in establishing a protection system that satisfies the requirements of 10 CFR 73.21. When applicable, Orders issued pursuant to authority granted by the AEA also contain with them the requirements and guidance for handling and protecting SGI. Also, the NRC has recently issued an SGI Designation Guide (September 2005) to assist licensees and other persons who possess SGI in making determinations about what information requires protection in accordance with 10 CFR Part 73.21 and Commission Orders authorized by the AEA. With respect to SUNSI the NRC has not provided guidance to other agencies. However, the NRC has issued two Regulatory Issue Summaries (RISs) to NRC licensees to assist them in identifying, handling, marking and protecting SUNSI. The RISs are: RIS 2005-26, "Control of Sensitive Unclassified Non Safeguards Information Related to Nuclear Power Reactors," dated November 7, 2005, and RIS 2005-31, "Control of Security-Related Sensitive Unclassified Non-Safeguards Information Handled by Individuals, Firms, and Entities Subject to NRC Regulation of the Use of Source, Byproduct, and Special Nuclear Material," dated December 22, 2005. Both RISs are available on the NRC's public website.</p>
Please provide a brief assessment of the effectiveness of your department or agency procedures for handling SBU or equivalent CUI data.	<p>The system for designation and protection of NRC's SGI has been in effect for over 20 years and is well understood by the nuclear industry and its regulators at the State and Federal level. Measures to enhance the protection of SGI (i.e., coversheets, designation guide, special Orders regarding SGI-M and mandatory web-based training) have increased overall compliance by the NRC staff and NRC licensees/stakeholders. The policies for marking, handling and protecting SUNSI at the NRC have been in effect for many years and were documented in NRC Management Directive 12.6. After September 11, 2001, the NRC reviewed its policies and consolidated 23 types of sensitive unclassified non-safeguards information into the current SUNSI groups based on similar handling, marking and protection criteria. There has been a learning curve as employees adjust to the new SUNSI groups, and SUNSI training has been provided to Headquarters NRC employees. A video tape of SUNSI training is available and planning is ongoing for a computer-based on-line SUNSI training module. In part, based on the lessons learned since initial implementation, the Commission is considering revisions to the current SUNSI policy.</p>

UNCLASSIFIED

UNCLASSIFIED

<p>Please provide any suggestions for standardizing or streamlining procedures for handling SBU or equivalent CUI data.</p>	<p>As part of its continued effort to enhance the effectiveness and efficiency of sensitive information protection, the NRC is implementing improved training and procedures. SGI is a specific statutory program. However, with respect to SUNSI, developing standards and common protocols for protecting SBU would be beneficial across the U.S. Government and the Nation. Authorizing legislation may be needed to provide a firm statutory basis and ensure consistent protection in the public and private sectors.</p>
---	--

UNCLASSIFIED

Section 2. Specific Categories of Information

This section applies to specific categories of SBU or equivalent CUI used by your department or agency. Please complete a separate table for each separate category of information.

Category Name	Safeguards Information	Point of Contact (name, phone, email)	Bern Stapleton, 301-415-2432, bws2@nrc.gov
Formal Definition	Information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed (1) control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; (2) security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; or (3) security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials covered by (1) and (2).		
Marking	Conspicuously mark the top and bottom of all pages with the SAFEGUARDS INFORMATION or SAFEGUARDS INFORMATION-MODIFIED HANDLING marking, depending on the type of material the information pertains to and the restrictions and requirements contained in 10 CFR Part 73 and/or Commission Orders. Place the name, title, organization, signature of the individual authorized to make an SGI or SGI-M determination, and the date and the basis for the SGI or SGI-M designation in the lower right corner of the face of the original document.		
Authority (law, regulation, policy, etc.) [Please enclose copies of reference documents if possible]	Authority is established in section 147 of the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2147, enacted as part of P.L. 96-295 (1980) . NRC regulations implementing these provisions are found in 10 CFR 73.21 (see http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0021.html). In addition, after September 11, 2001, pursuant to authority granted by the AEA, the NRC issued several Orders pertaining to Safeguards Information to various classes of licensees.		
Is this category of information used only by specific elements within your department, or does it apply agency-wide? Is it recognized broadly across the U.S. Government?	A large number of NRC employees, other Federal agencies' employees with homeland security responsibilities, employees and contractors of the regulated industry, states and local agency employees and contractors and participants in NRC adjudications need and have access to and may potentially generate Safeguards Information. SGI is unique to the NRC under the Atomic Energy Act of 1954, as amended, but is binding across the U.S. Government.		
Who is authorized to apply this designation?	NRC personnel are authorized to make SGI determinations provided they have received the required SGI designation training and certification from NRC's Information Security Section. Within contractor organizations, the NRC contracting office's representative or the NRC project officer, when necessary, authorizes employees to perform this function. NRC licensees or others responsible for the protection of SGI are also authorized to make SGI determinations in accordance with the criteria contained in 10 CFR 73.21.		

UNCLASSIFIED

UNCLASSIFIED

Section 2. Specific Categories of Information

Who is authorized to remove the designation? What criteria are used?	Any individual authorized to determine that a document contains SGI may remove such markings when the information no longer meets the criteria outlined in 10 CFR 73.21 or Commission Orders. If such a determination is made, the following individuals are required to be informed of the decision: the originator of the document; his or her successor; or a supervisor of either.
Are there provisions for automatic removal of the designation after a specified time?	No. As was stated in the answer to the previous question, SGI markings may be removed when the information no longer meets the criteria outlined in 10 CFR 73.21.
Are there any special restrictions on access to this category of information, by agencies or individuals?	Yes. The criteria for individuals to be allowed access to SGI are contained in 10 CFR 73.21, "Access to Safeguards Information," and in certain Orders issued by the commission.
Are there any special provisions governing access to this information by State, local, or tribal governments or private sector entities?	Yes. Special provisions for access to SGI by State, local, and tribal governments or private sector entities are also contained in 10 CFR 73.21, "Access to Safeguards Information," and in certain Orders issued by the Commission.
Describe any procedures for processing, storing, tracking, or disseminating this category of SBU or equivalent CUI, including any special requirements that apply to automated information systems.	The NRC does not track documents containing SGI by serial number or other designation. Documents containing SGI, protected pursuant to the requirements contained in Part 73, are required to be stored in security storage containers, as defined in 10 CFR 73.2, when not in use. SGI may be processed, stored, or produced on stand-alone desktop computers or laptops. SGI shall not be processed, stored, or produced on any computer connected to the NRC unclassified local area network (LAN). Only SGI files that are properly encrypted in accordance with the National Institute of Standards and Technology Federal Information Processing Standards 140-2, "Security Requirements for Cryptologic Modules," may use the computers connected to the NRC unclassified LAN to transmit the encrypted SGI file by e-mail to authorized recipients. Unprotected circuits may be used to transmit SGI only under emergency or extraordinary conditions (e.g., circumstances that require immediate communication in order to report, summon assistance for, or respond to a safeguards event or an event that has potential security significance.) SGI protected pursuant to requirements set forth in Commission Orders and marked SGI-M may have separate modified requirements.
Describe procedures for marking this category of SBU. Is information marked at the document or paragraph level?	Documents containing SGI or SGI-M must be conspicuously marked at the top and bottom of all pages with the SAFEGUARDS INFORMATION or SAFEGUARDS INFORMATION-MODIFIED HANDLING marking. Place the name, title, organization, signature of the individual authorized to make an SGI or SGI-M determination, and the date and the basis for the SGI designation in the lower right corner of the face of the original document. See NRC Management Directive and Handbook 12.6, "NRC Sensitive Unclassified Information Security Program" for more detailed procedures on marking SGI. Portion marking is required when a document contains several categories of SBU in order to distinguish SGI or SGI-M portions (e.g., paragraphs, pages, and appendices) from those other categories. Otherwise, the information is marked at the document level only. Please note that it is necessary to distinguish SGI or SGI-M portions from unclassified/uncontrolled portions.

UNCLASSIFIED

Section 2. Specific Categories of Information

Describe any training or guidance given to department or agency employees regarding marking, storing, or handling of this category of SBU.

The NRC has implemented an agency-wide information security awareness training program to ensure that NRC employees and contractors, including individuals making SGI determinations, are aware of agency requirements and policies governing SGI. Completion of this training is an annual requirement for all employees. NRC ensures that employees and designated contractors take such training, which is web-based. NRC employees and designated contractors who have the authority to designate information as SGI are required to complete additional information security awareness training that specifically addresses SGI in more detail. For those who handle SGI outside the NRC (licensees and stakeholders) the NRC has made available a "Designation Guide for Safeguards Information" to assist licensees and other persons in making determinations about what information requires protection in accordance with 10 CFR Part 73.21 and Commission Orders issued pursuant to authority granted by the AEA.