

UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS  
WASHINGTON, D.C. 20555-0001

December 22, 2005

**NRC REGULATORY ISSUE SUMMARY 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**

**ADDRESSEES**

All licensees, certificate holders, applicants, and other entities (hereafter referred to as "licensees and others") subject to regulation by the U.S. Nuclear Regulatory Commission (NRC) of the use of source, byproduct, and special nuclear material, except for those as covered by provisions of Regulatory Issue Summary (RIS) 2005-26 for nuclear power reactors.

**INTENT**

This RIS sets forth procedures that licensees and others are encouraged to follow when handling documents and/or when submitting documents to the NRC that contain security-related sensitive information, other than classified or safeguards information, that could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack. Attached to this RIS are screening criteria that licensees and others should use to identify security-related sensitive information.

No specific action nor written response is required.

**BACKGROUND**

NRC traditionally has given the public access to a significant amount of information about the facilities and materials the Agency regulates. Openness has been and remains a cornerstone of NRC's regulatory philosophy. The Atomic Energy Act, subsequent legislation, and various NRC regulations have given the public the right to participate in the licensing and oversight process for NRC licensees. To participate in a meaningful way, the public must have access to information about the design and operation of regulated facilities and use of nuclear materials. However, NRC and other Government agencies have always withheld some information from public disclosure for reasons of security, personal privacy, or commercial or trade secret protection.

**ML053480073**

In the post-September 11, 2001, environment, NRC, like many other agencies, has found it necessary to be more judicious in determining what information to voluntarily release, so as not to inadvertently provide assistance to those who might use certain information for malevolent acts. NRC has issued orders and advisories and taken specific actions regarding the security of its licensed facilities and has also assessed and revised its policies and practices for making information available to the public. One of the actions NRC took was to suspend public access to documents in its electronic Agency-wide Documents Access and Management System (ADAMS) on October 25, 2004. Subsequently, NRC screened those documents to determine whether they contained security-related sensitive information. Based on this screening, a large number of documents were returned to public access in ADAMS. This screening process continues as requests for specific documents are received and as new documents are created by NRC and received from licensees and others.

To facilitate this screening process, NRC has developed screening criteria for conducting its reviews. In November 2005, NRC issued guidance (NRC RIS 2005-26) for assessing whether documents associated with reactor licensees should be made publicly available. As part of the continuing efforts in this area, NRC has now developed the attached criteria for screening from public disclosure security-related sensitive information associated with various NRC-regulated activities of persons handling source, byproduct, and special nuclear material.

This RIS and its attachments do not apply to classified information or Safeguards Information. Classified information (Confidential, Secret, Top Secret) is withheld from the public by law. Safeguards Information is withheld because it provides details of security measures at nuclear facilities. Handling requirements for classified information and Safeguards Information are set forth in various NRC orders, regulations, and generic communications (e.g., requirements for the handling and protection of Safeguards Information are discussed in RIS-2003-08, "Protection of Safeguards Information from Unauthorized Disclosure," dated April 30, 2003).

Sensitive (but unclassified, non-safeguards) information covers a range of information for which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, commercial or financial interests of an entity, the conduct of NRC and Federal Programs, or the personal privacy of individuals. As noted above, this RIS covers security-related information which, if released, could cause harm to the public interest as it could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack. Specifically, information that should be protected under this RIS is described in Attachment 2. In addition, licensees and others should use the procedures set forth below to protect information designated for protection by other federal, State, or local agencies.

## **SUMMARY OF ISSUE**

This RIS:

- 1) Informs licensees and others of the screening criteria that NRC uses to identify and protect security-related sensitive information in documents generated by the Agency and in documents received from licensees and others;
- 2) Encourages licensees and others to identify security-related sensitive information contained in documents submitted to NRC, by using the screening criteria in Attachment 2 and marking procedures; and

- 3) Encourages licensees and others that may possess security-related sensitive information to control the information, to limit the risk that the information might fall into the hands of those who would use it for malevolent acts.

Specifically, protection of the information should be implemented in the following manner:

1. Screening of Future Documents Submitted to NRC

To assure that future submittals containing security-related sensitive information are not made publicly available in ADAMS, while still making other appropriate information available to the public, NRC is encouraging licensees and others to screen submittals in accordance with the guidance in Attachment 2. If practical, documents submitted to NRC should avoid including security-related sensitive information to permit releasing the document to the public in its entirety.

2. Marking and Submitting Documents Containing Security-Related Sensitive Information

If it is necessary to include security-related sensitive information in a submitted document, the submittal should be marked to indicate the presence of such information as follows:

- a) The cover letter should clearly state that the attached documents contain security-related sensitive information. When separated from the attached documents, if the cover letter itself does not contain security-related sensitive information, the cover letter itself is uncontrolled.
- b) As shown in Attachment 1 (Section A), the top of every page of a letter or document that contains security-related sensitive information should include the marking "Security-Related Information — Withhold Under 10 CFR 2.390" (note that NRC's procedure for these documents is to mark them as "Official Use Only - Security-Related Information"). For the pages having security-related sensitive information, an additional marking (e.g., an editorial notebox) should be included adjacent to the material meeting the screening criteria in Attachment 2.

Information on suggested handling and methods of submittal of security-related sensitive information is also contained in Attachment 1 (Section B).

Licensees and others can submit both a public and a non-public version of a document, when security-related documents need to be submitted. The public version could have the security-related sensitive information "marked out" or removed with a notation that the information was withheld on the basis that it is "Security-Related Information." This is similar to what is sometimes done to protect proprietary information under 10 CFR 2.390, except that an affidavit is not needed. Alternatively, security-related sensitive information could be segregated from the main body of the document and included only in attachments to the submittal. Only the attachments containing security-related sensitive information would be marked for withholding from public disclosure. Using this approach, the public version need not be marked as containing security-related sensitive information.

### 3. Protection of Security-Related Sensitive Information

Documents that contain security-related sensitive information should be protected from public disclosure, using methods similar to that for protecting proprietary information. To the extent practicable, any existing documents containing security-related sensitive information that licensees or others have previously made available to the public should be withdrawn from public access. As with proprietary information, licensees and others should have sufficient internal controls to prevent release of information. Possible methods to prevent the inadvertent release of security-related sensitive information include marking documents "Security-Related Information - Withhold Under 10 CFR 2.390," restricting access to electronic recordkeeping systems that contain such information, and controlling the reproduction, distribution, and destruction of potentially sensitive records. Licensees and others should ensure that similar controls are in place when security-related sensitive information is provided to outside parties such as contractors or other Government agencies, and that the information is made available only to such parties who have a need to know the information to perform their jobs and who are made aware of the security-related nature of the information.

This RIS, the attached screening criteria, and additional explanatory material, as appropriate, are also posted on the NRC Web site at <http://www.nrc.gov/reading-rm/sensitive-info.html>) (note that the criteria for fuel cycle facilities in this website and in this RIS supercedes information at <http://www.nrc.gov/materials/fuel-cycle-fac/review-criteria-fuel-cycle.html>).

The NRC staff will interact with licensees and others on a case-by-case basis to resolve questions regarding the application of the procedures and screening criteria set forth in this RIS and its attachments.

NRC will continue to make available to the public as much information as possible. Much of NRC's information is readily available to the public via the NRC Web site ([www.nrc.gov](http://www.nrc.gov)) and NRC's ADAMS system ([www.nrc.gov/reading-rm/adams.html](http://www.nrc.gov/reading-rm/adams.html)). In addition, other information may be released to the public in response to formal and/or informal requests. Although the security-related sensitive information screening criteria were developed with the principles of the Freedom of Information Act (FOIA) in mind, a review for security-related sensitive information does not substitute for a FOIA review. FOIA requests will continue to be reviewed and processed independently from the security-related sensitive information review process.

#### **BACKFIT DISCUSSION**

This RIS requires no action nor written response and is, therefore, not a backfit under 10 CFR 70.76, 72.62, or 76.76. Consequently, the NRC staff did not perform a backfit analysis.

#### **FEDERAL REGISTER NOTIFICATION**

A notice of opportunity for public comment on this RIS was not published in the *Federal Register* because it is informational and does not represent a departure from current regulatory requirements and practice.

## **SMALL BUSINESS REGULATORY ENFORCEMENT FAIRNESS ACT OF 1996**

NRC has determined that this action is not subject to the Small Business Regulatory Enforcement Fairness Act of 1996.

## **PAPERWORK REDUCTION ACT STATEMENT**

This RIS does not contain information collections and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, et seq.).

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

[/RA/](#)  
Charles L. Miller, Director  
Division of Industrial and Medical  
Nuclear Safety  
Office of Nuclear Material Safety  
and Safeguards

### Technical Contacts:

<u>Materials IMNS/Regional</u>	<u>Spent Fuel Storage and Transportation</u>	<u>Fuel Cycle</u>
Paul Goldberg, NMSS/IMNS 301-415-7842 E-mail: pfg@nrc.gov	Joe Sebrosky, NMSS/SFPO 301-415-1132 E-mail: jms3@nrc.gov	Patricia Silva, NMSS/FCSS 301-415-8029 E-mail: pas6@nrc.gov
<u>Decommissioning</u>	<u>HLWRS</u>	<u>Import/Export</u>
Ted Carter, NMSS/DWMEP 301-415-6668 E-mail: thc1@nrc.gov	Alexander Sapountzis 301-415-7822 E-mail: aps@nrc.gov	Stephen Dembek 301-415-2342 E-mail: sxd@nrc.gov

### Attachments:

1. Suggested Markings; Withhold From Public Disclosure in Accordance With 10 CFR 2.390
2. NMSS Guidance on Screening Criteria for Security-Related Sensitive Unclassified Non-Safeguards Information
3. List of Recently Issued NMSS Generic Communications

**SMALL BUSINESS REGULATORY ENFORCEMENT FAIRNESS ACT OF 1996**

NRC has determined that this action is not a rule and thus is not subject to the Small Business Regulatory Enforcement Fairness Act of 1996.

**PAPERWORK REDUCTION ACT STATEMENT**

This RIS does not contain information collections and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, et seq.).

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

[/RA/](#)  
Charles L. Miller, Director  
Division of Industrial and Medical  
Nuclear Safety  
Office of Nuclear Material Safety  
and Safeguards

Technical Contacts:

<u>Materials IMNS/Regional</u>	<u>Spent Fuel Storage and Transportation</u>	<u>Fuel Cycle</u>
Paul Goldberg, NMSS/IMNS 301-415-7842 E-mail: pfg@nrc.gov	Joe Sebrosky, NMSS/SFPO 301-415-1132 E-mail: jms3@nrc.gov	Patricia Silva, NMSS/FCSS 301-415-8029 E-mail: pas6@nrc.gov
<u>Decommissioning</u>	<u>HLWRS</u>	<u>Import/Export</u>
Ted Carter, NMSS/DWMEP 301-415-6668 E-mail: thc1@nrc.gov	Alexander Sapountzis 301-415-7822 E-mail: aps@nrc.gov	Stephen Dembek 301-415-2342 E-mail: sxd@nrc.gov

Attachments:

1. Suggested Markings; Withhold From Public Disclosure in Accordance With 10 CFR 2.390
2. NMSS Guidance on Screening Criteria for Security-Related Sensitive Unclassified Non-Safeguards Information
3. List of Recently Issued NMSS Generic Communications

DISTRIBUTION:

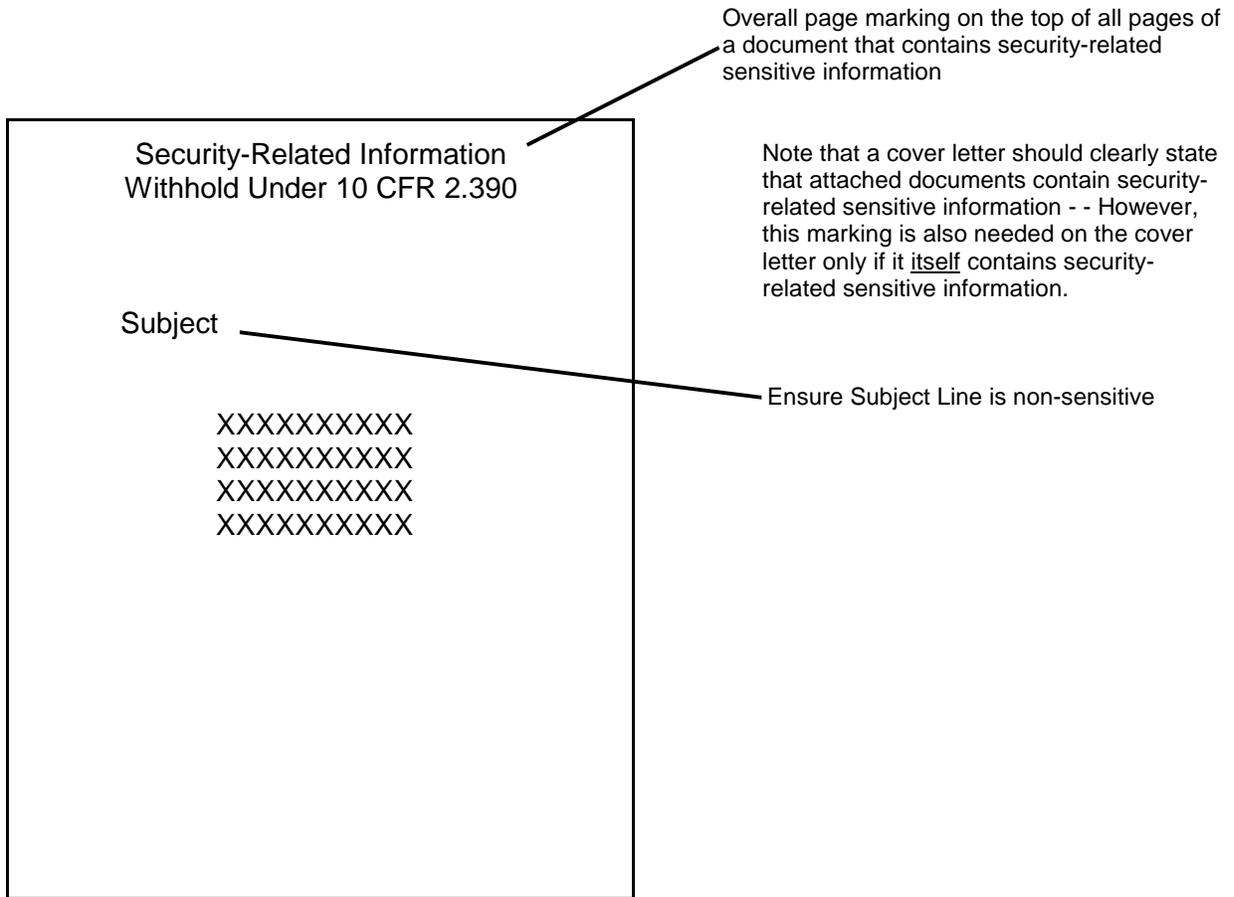
**ML053480073**

OFFICE	IMNS/RGB	IMNS/MSIB	TECH ED	IMNS/RGB	IMNS/RGB
NAME	FCardile	AMcIntosh	EKraus	CAbrams	SMoore
DATE	12/12/05	12/15/05	12/8/05	12/20/05	12/21/05
OFFICE	D:SFPO	D:FCSS	D:HLWRS	D:DWMEP	OIS
NAME	WBrach	RPierson	WReamer	LCamper	BShelton
DATE	12/19/05	12/20/05	12/19/05	12/19/05	12/20/05
OFFICE	D:IP	D:STP	NSIR	OGC	D:IMNS
NAME	JDunnLee	JSchlueter	MWeber	TRothschild	CMiller
DATE	12/20/05	12/21/05	12/19/05	12/16/05	12/22/05

## SUGGESTED MARKINGS AND HANDLING

This attachment provides information on suggested markings for pages of a document that contains security-related sensitive information (Section A) and suggested handling of such documents (Section B).

### A. Page Markings



B. Appropriate Controls for Handling Documents

- Access: Need-to-know in order to perform official licensee, applicant or entity functions.
- Storage: Openly within licensee, applicant, or other entity facilities with electronic or other access controls, for example, key cards, guards, alarms.
- Mail: U.S. Postal Service first class mail, registered mail, express mail, or certified mail in single opaque envelope with no external markings to indicate 10 CFR 2.390 contents.
- Electronic Transmission: Over phone if the recipient is confirmed as being authorized to access the information; over facsimile if it is confirmed that a recipient who is authorized to access the information will be present to receive the transmission; over encrypted computer e-mail (using computer software such as SecureZip).

Note that NRC is using SecureZip when transmitting security-related sensitive information by e-mail to licensees and others to encrypt electronic information. Users will be prompted for a password to access a free download of the reader.