COMSECY-05-0054

October 26, 2005

MEMORANDUM TO: Those on the Attached List

FROM: Luis A. Reyes **/RA/**
Executive Director for Operations

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION (SUNSI)

In a memorandum to you dated January 19, 2005, I directed that the recommendations of the SUNSI task force be implemented by a staff working group supported by the offices and chaired by the Office of Information Services. The interoffice working group completed the requested work and identified numerous key changes on how the Agency handles SUNSI. All of those changes are identified in the attached Communication Plan, with the significant changes listed below. The new policy:

Eliminates the need for all cover sheets except for Allegation Information and Investigation Information;
Requires marking of header and footer for each type of SUNSI;
Determines that portion marking of documents is not required; and
Notes that SUNSI must be encrypted when transmitted electronically.

I am implementing the new policy and procedures effective on the date of this memorandum. The attached "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" describes the new policy and procedures which will be incorporated in the next revision of Management Directive 12.6. Additionally, over the next four months, SUNSI awareness training sessions will be held in the Auditorium. Staff should take advantage of these training sessions to become familiar with the new policy. Further training will be incorporated into the Computer Based Learning (CBT) class on Information Computer Security in the spring of 2006.

Attachments: As stated

MEMORANDUM TO THOSE ON THE ATTACHED LIST DATED: October 26, 2005

SUBJECT: POLICY REVISION: HANDLING, MARKING, AND PROTECTING SENSITIVE UNCLASSIFIED NON-SAFEGUARDS INFORMATION (SUNSI)

	Mail Stop	
	O-16	C1
John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste	T-2	E26
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel	T-3	F23
Karen D. Cyr, General Counsel	O-15	D21
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication	O-16	C1
Jesse L. Funches, Chief Financial Officer	T-9	F4
Hubert T. Bell, Inspector General	T-5	D28
Janice Dunn Lee, Director, Office of International Programs	O-4	E21
William N. Outlaw, Director of Communications	O-16	C1
Rebecca L. Schmidt, Director, Office of Congressional Affairs	O-16	C1
Eliot B. Brenner, Director, Office of Public Affairs	O-2	A13
Annette Vietti-Cook, Secretary of the Commission	O-16	C1
Luis A. Reyes, Executive Director for Operations	O-16	E15
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO	O-16	E15
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO	O-16	E15
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO	O-16	E15
William M. Dean, Assistant for Operations, OEDO	O-16	E15
Timothy F. Hagan, Director, Office of Administration	T-7	D26
Michael R. Johnson, Director, Office of Enforcement	O-14	E1
Guy P. Caputo, Director, Office of Investigations	O-3	F1
Edward T. Baker, Director, Office of Information Services	T-6	F15
James F. McDermott, Director, Office of Human Resources	T-3	A2
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights	T-2	D56
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards	T-8	A23
James E. Dyer, Director, Office of Nuclear Reactor Regulation	O-5	E7
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research	T-10	F12
Janet R. Schlueter, Director, Office of State and Tribal Programs	O-3	C10
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response	T-4	D22a
Samuel J. Collins, Regional Administrator, Region I	RGN-I	
William D. Travers, Regional Administrator, Region II	RGN-II	
James L. Caldwell, Regional Administrator, Region III	RGN-III	
Bruce S. Mallett, Regional Administrator, Region IV	RGN-IV	

NRC Policy For
Handling, Marking, and Protecting
Sensitive Unclassified Non-Safeguards Information

A. Purpose and Scope

This policy is issued to ensure that sensitive unclassified non-safeguards information (SUNSI) is properly handled, marked, and adequately protected from unauthorized disclosure.

"SUNSI" means any 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.

The various categories of SUNSI have been organized into the following seven groups:

- Allegation information
- Investigation information
- Security-related information
- Proprietary information
- Privacy Act information
- Federal-, State-, foreign government-, and international agency-controlled information
- Sensitive internal information

To the extent that requirements under a section for a particular SUNSI group were already stipulated in a statute, regulation, or other directive, the requirements have been incorporated into this policy. The requirements set forth in this policy and procedures for handling allegation information come from Management Directive (MD) 8.8, "Management of Allegations." The requirements for the handling of Privacy Act information come from the Privacy Act of 1974, as amended, and MD 3.2, "Privacy Act." The requirements for marking incoming confidential commercial or financial (proprietary) information come from 10 CFR 2.390.

When more than one SUNSI group applies to information, the most restrictive handling requirement of the applicable groups should be applied.

B. Applicability

NRC employees, consultants, and contractors are responsible for ensuring the procedures specified in this announcement are followed to protect SUNSI. The use of the word "contractors" includes subcontractors.

C. Handling Requirements for SUNSI

1. Web Address for Handling Requirements

The handling requirements for SUNSI are published on the NRC internal Web site at http://www.internal.nrc.gov/sunsi/. The Web site contains detailed requirements for each of seven SUNSI groups in the following fourteen areas.

a. Applicable document categories
b. Authority to designate
c. Access
d. Marking
e. Cover sheet
f. Reproduction
g. Processing on electronic systems
h. Use at home
I. Use while traveling or commuting
j. Physical copy transmission
k. Electronic copy transmission
l. Storage
m. Destruction
n. Decontrol authority

2. Change requests

SUNSI handling requirements will be maintained and updated as needed at the SUNSI Web site. Changes will be announced to the NRC staff.

Requests to add additional document categories to a SUNSI group and other proposed changes should be submitted in writing to the Director, Information and Records Services Division, Office of Information Services. The request should state specifically where the addition or change should be made and a justification why the addition or change is needed.

D. Generally Applicable Requirements

1. Marking

Each document containing SUNSI must be properly and fully marked when such markings are required for the particular SUNSI group. (See item 4, Marking, in the SUNSI group handling requirements http://www.internal.nrc.gov/sunsi/.)

2. Need-To-Know Access

A security clearance is not required for access to SUNSI. However, except as authorized by the Commission, no person, including employees of the U.S. Government, NRC, an NRC licensee or certificate holder, or an employee, agent, or contractor of a license applicant may have access to SUNSI unless: (1) that

person has an authorized need to know, and (2) the information is for the conduct of official agency business.

If doubt exists in any particular case whether it is proper to grant access to SUNSI originating from outside the NRC, consult with the originating party, the party, or other source from which the information was derived.

3. Ensuring legible markings on copies

All copies must clearly show the protective markings on the original document. Markings on documents submitted for reproduction should be in black or red and dark enough to be reproduced legibly.

4. Packaging SUNSI for Transmission

Material used for packaging SUNSI for physical transmission must be opaque and of such strength and durability as to provide secure protection for the document in transit, prevent items from breaking out of the container, and facilitate the detection of any tampering with the container.

5. Profiling SUNSI in ADAMS

When a document containing SUNSI is authorized to be entered into the Agencywide Documents Access and Management System (ADAMS), personnel entering the document must ensure that one of the sensitive values (Sensitive or Sensitive-Copyright, as appropriate) is marked in the "Document Sensitivity" profile property and that the "Availability" profile property is marked as "Non-Publicly Available." Identifying the appropriate document sensitivity and availability along with the markings on the documents will aid in protecting SUNSI. It will also alert staff to the sensitivity of the document when it is requested under Freedom of Information Act or the Privacy Act, thus ensuring that the document is properly reviewed under FOIA and Privacy Act exemptions standards.

6. Removal of Markings

Normally a document will retain its markings until the agency decides that the document will be made public either on its own discretion, or in response to a FOIA request. Before releasing a document with a SUNSI marking, the marking on the copy to be released should preferably be blackened out, or at a minimum, marked through in such a way that it conveys that the marking is no longer applicable to the document. This should be done on each page containing a marking.

7. Inadvertent or Unauthorized Release of SUNSI

Whenever SUNSI is inadvertently released or disclosed by the NRC or its contractors, the office director must promptly inform the Executive Director for Operations (EDO) and the Office of the Inspector General (OIG) in accordance with MD 3.4, "Release of Information to the Public." If the inadvertent release occurs via ADAMS or NRC's public web site, the ADAMS Support Center (415-1234, select manual option 1) must be immediately notified.

8. Release of Information to the Public

Each document considered for routine release to the public by the agency must be reviewed to determine whether the document is releasable under NRC policy (See MD 3.4, "Release of Information to the Public") including application of screening criteria for determining if information should be withheld from public disclosure because it could reasonably be expected to be useful to a potential adversary. (See http://www.internal.nrc.gov/NRC/Guidance/index.html.) Each document requested by the public via the Freedom of Information Act or Privacy Act must be reviewed to determine whether the document, or part thereof, is releasable or is exempt from public disclosure. (See MD 3.1, "Freedom of Information Act" and MD 3.2, "Privacy Act.")

The presence or absence of cover sheets or markings as "Allegation Information," "Investigation Information," or similar markings, does not determine whether a document may be withheld from the public. Whenever an NRC employee has a question regarding the releasability of information, the employee should consult with the employee's supervisor or—

- The Information and Records Services Division (IRSD), Office of Information Services (OIS) if a request for information involves the Freedom of Information Act (FOIA) or the Privacy Act. (See MD 3.1, "Freedom of Information Act" and MD 3.2, "Privacy Act.")

- The Office of Enforcement (OE) regarding allegation information.

- The Office of Investigations (OI) regarding OI investigation information.

- The Office of the Inspector General (OIG) regarding OIG investigation information.

- The Office of Nuclear Reactor Regulation (NRR) or the Office of Nuclear Material Safety and Safeguards (NMSS), as appropriate, on whether a document contains 10 CFR 2.390(d)(1) information.

- The Office of the General Counsel (OGC), or appropriate regional counsel, on legal questions.

Other Government and International agencies should be consulted before documents bearing restrictive markings or containing SUNSI of primary interest to them are released to the public.

9. "No Comment" Policy for SUNSI

Should SUNSI appear in the public domain (e.g. newspapers) prior to the agency's official release of that information, and should an NRC employee be contacted by an organization outside of the agency to confirm or deny either the accuracy or sensitivity of the released information, NRC employees should respond to such a request with a "no comment" statement. If an NRC employee has any questions about how to handle a request for comment about an unauthorized release of SUNSI, the employee should consult with the employee's supervisor or the originator of the information.

10. Security Preparations Required for Hearings, Conferences, or Discussions

NRC personnel, NRC consultants, NRC contractor personnel, and others (e.g., bidders) who arrange or participate in hearings, conferences, or discussions (see MD 3.5, "Attendance at NRC Staff Sponsored Meetings") involving SUNSI shall—

- Ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed.
- Inform participating personnel that the specific information they will receive is SUNSI and advise them of the protective measures required.
- Ensure that no discussion takes place that is audible or visible to persons not authorized access to the information.

11. Contact for SUNSI Policy

Questions regarding SUNSI and associated policy should be addressed to OIS/IRSD/FOIA/Privacy Team.