# 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" refers to 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 nine groups:

- Allegation information
- Investigation information
- Critical Electric Infrastructure Information (CEII)
- Export Controlled Information (ECI)
- 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. Requirements for electronic processing, storage, destruction, and transmission of SUNSI can be found in MD 12.6.

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

Web Address for Handling Requirements

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

- Applicable document categories
- Authority to designate
- Access
- Marking
- Cover sheet
- Reproduction
- Processing on electronic systems
- Use at home
- Use while traveling or commuting
- Physical copy transmission
- Electronic copy transmission
- Storage
- Destruction
- Decontrol authority

## D. Generally Applicable Requirements

1. Marking

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

2. Need-To-Know Access

   A security clearance is not required for access to SUNSI. However, except as the Commission may otherwise authorize, 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 that person has an established need-to-know the information for conducting official business.

   If doubt exists in any particular case whether it is proper to grant access to SUNSI originating from outside the NRC, NRC contractors, or NRC licensees or applicants, consult with the originating party, the party responsible for the information, or other source from which the information is 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 Physical 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 (e.g., **Sensitive- Security Related – Periodic Review Required, Sensitive- Proprietary, Sensitive- Protected subject to adjudicatory order, etc.**) 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 the Freedom of Information Act (FOIA) 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 NRC personnel or contractors, a security incident has occurred. Some examples of SUNSI-related security incidents include leaving sensitive unclassified documents or material unattended, unsecured, or improperly stored (including on shared network drives unless access controls are applied); improper transmission of sensitive unclassified documents or material; allowing an unauthorized person access to sensitive unclassified information; and/or failure to safeguard a sensitive unclassified lock combination.

In the event of a SUNSI security incident, in accordance with MD 3.4, "Release of Information to the Public," the office director shall promptly inform the Executive Director for Operations (EDO) and the Office of the Inspector General (OIG).

In accordance with MD 12.1, "NRC Facility Security Program," NRC employees and contractors shall report all security incidents immediately following their occurrence or observed occurrence by:

A. Completing and submitting an NRC Form 183, "Report of Security Incident." If necessary, the initial report to the Division of Facilities and Security (DFS) may be made orally but must be finalized in writing by submitting an NRC Form 183 to DFS. A report should not contain any SGI or classified information unless the report is protected according to the level of information involved when transmitted or verbally communicated to DFS through an authorized secure telecommunications system or secure information technology (IT) system. A security incident may be initially reported by telephone to 301-415-6885, or online at http://drupal.nrc.gov/content/report-safety-or-security-incident.

B. A contractor shall immediately report a security incident to DFS and send a copy to the NRC project officer and/or Contract Officer Representative (COR) and the regional security advisor, if appropriate. The report must include the details of the incident, as well as the name of the person who committed it. If the contractor does not have the capability to complete and submit the NRC Form 183, the COR must do so on behalf of the contractor.

C. The NRC Form 183 must contain the following:
   1) The full name of the individual involved;
   2) The individual's office and title or if a contractor, the company and COR's name;
   3) The classification of the information involved, but not the vulnerability if it has not been corrected; and
   4) The date, reason or cause, and nature of the incident.

8. Consequences of non-compliance with protecting SUNSI

Consequences of non-compliance with protecting SUNSI may include:

A. Removal of system access for a specified period of time;

B. Mandated training regarding the information about the specific security incident; and/or

C. Possible disciplinary action up to and including removal from Federal service or the contract. (See MD 12.1, "NRC Facility Security Program," and MD 12.5, "NRC Cybersecurity Program").

9. 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://drupal.nrc.gov/sunsi/34661).) Each document requested by the public via FOIA or the 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 Governance & Enterprise Management Services Division (GEMSD), Office of the Chief Information Officer (OCIO) 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.

10. <u>“No Comment” Policy for SUNSI</u>

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, the NRC employee 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.

11. 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.