GUIDANCE TO LICENSEES FOR THE HANDLING OF SENSITIVE UNCLASSIFIED INFORMATION AND OFFICIAL USE ONLY INFORMATION

The U. S. Nuclear Regulatory Commission (NRC) considers that any information that could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack should be withheld from public disclosure.

NRC has determined that the proposed Protective Measures (PMs), Implementing Guidance, and Regulatory Issue Summary (RIS) Threat Conditions Table are sensitive unclassified information, which will be handled as Official Use Only (OUO). The NRC will not publicly disclose this information except as required by law.

Each licensee must protect this information from unauthorized release to the public. Additional information and guidance on how to protect this information are provided below. Similarly, a licensee has a vested interest in protecting its own security, confidential commercial, or financial information and would only reveal it to those persons who the licensee has determined that they need the information to conduct business. NRC expects this guidance to be compatible with licensees' information protection strategies.

PROTECTING OFFICIAL USE ONLY AND OTHER SENSITIVE UNCLASSIFIED INFORMATION FROM RELEASE TO THE PUBLIC

OFFICIAL USE ONLY (OUO) INFORMATION: OUO information is sensitive unclassified information, generated by a U.S. Government Agency, that (1) may fall under the Freedom of Information Act exemptions and (2) has the potential to damage government, commercial, or private interests if disseminated to persons who do not need the information to perform official activities.

ACCESS: Individuals having access to OUO or other sensitive unclassified Information must have the appropriate "need to know." The NRC will only furnish sensitive unclassified information to those persons who need the information to conduct official business. Further dissemination of sensitive-unclassified, physical-protection-measures information should be limited to individuals that have a need to know a licensee's security information. If a licensee has questions about who should have access to sensitive unclassified information they should consult with the NRC office originating the information, the office that has primary interest in the information, or the original source from which the information was derived to determine "need to know."

WHEN SENSITIVE UNCLASSIFIED INFORMATION INFORMATION IS MARKED: A U.S. Government Agency marks a document as OUO when it is essential to ensure proper handling and to ensure that all persons having access to the record are aware that the document is not to be publicly released and only distributed to those who have a "need to know" to conduct official business. When NRC provides sensitive unclassified information to licensees or other non-government persons with a need to know, it would be marked as **"Exempt from Public Disclosure in Accordance with 10 CFR 2.390".**

MARKINGS: OUO documents are marked at the top and bottom of the page on the face of each document containing the sensitive information for "Official Use Only" when the marking is required to ensure proper handling. Similarly, sensitive unclassified information sent to

licensees would be marked **"Exempt from Public Disclosure in Accordance with 10 CFR 2.390".**

FILES OR FOLDERS: The front and back of folders containing OUO information should be marked with "Official Use Only" or other similar marking for easy identification and to ensure proper handling.

TRANSMITTAL DOCUMENTS: Documents that do not in themselves contain sensitive unclassified information but are used to transmit one or more documents containing this information are marked to indicate the fact that sensitive unclassified information is contained in the documents transmitted. The markings, "OFFICIAL USE ONLY" or **"Exempt from Public Disclosure in Accordance with 10 CFR 2.390,"** indicating the category of information is placed at the top and bottom of only the first page of the transmitted document. In addition, the following marking is placed at the side or bottom on the first page of the transmittal document: "Document transmitted herewith contains sensitive unclassified information. When separated from enclosures, this document is decontrolled."

COVER SHEETS: Cover Sheets should be used for sensitive information when their use facilitates identification or protection of the information.

REPRODUCTION: A minimum number of copies of documents containing or said to contain sensitive unclassified information may be reproduced by holders to meet operational requirements without permission of the originator or responsible office. Care must be taken to prevent unauthorized access during reproduction and in the disposition of documents containing sensitive unclassified information.

PREPARATION FOR TRANSMISSION: Documents containing sensitive unclassified information must be addressed to an individual authorized access to that information. Material used for packing 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.

TRANSMISSION: Documents containing sensitive unclassified information must be transmitted, using a single opaque (sealed) envelope, by one of the following methods:

1. Messenger, contractor authorized messenger or courier,
2. U.S. Postal Service First Class Mail,
3. Registered Mail, Express Mail or Certified Mail, if tracking and delivery verification are desired, or
4. Interoffice mail or pouch mail

If hand carrying the document must be in the couriers possession at all times. At no time may the document be left unattended or unsecured while in transit.

RECEIPTS: Notifications for receipt of a transmitted sensitive information documents are not required. A receipt may be utilized if the sender wishes to ensure the delivery of the document(s).

TELECOMMUNICATIONS: Utmost discretion must be used in the transmission of any sensitive unclassified information by electrical means. Mail channels are preferred. Official Use Only information must be encrypted if encryption is requested by the sender.

AUTOMATIC DATA PROCESSING: Sensitive unclassified information may be processed or produced on an Automated Information System (AIS) provided that the system is authorized for the generation of OUO information and the user is appropriately briefed on the proper security procedures to utilize while using the computer system. Individuals must protect the information during use by maintaining control and by ensuring only individuals with the appropriate "need to know" have access to the information.

STORAGE: NRC recommends that if a facility has an electronic access control system in place or contract guards on duty there are no additional storage requirements necessary for licensees' sensitive security information related to physical protection information. If these security measures are not available, additional protection (locked cabinet, desk, office, etc.) is required due to the sensitivity of the information requiring protection.

DESTRUCTION: Recipients of sensitive unclassified information documents are responsible for destroying these documents when they are no longer required. Records of destruction are not required. Documents containing sensitive unclassified information must be destroyed by a method that will prevent reconstruction of the information. Documents may be destroyed by tearing them into small pieces or by burning, pulping, pulverizing, shredding, or chemical decomposition. (Note: OUO or other sensitive unclassified information should not be sent to recycling without being destroyed first)

REMOVAL OF INFORMATION FROM THE SENSITIVE UNCLASSIFIED CATEGORY: Periodic review of documents containing sensitive unclassified information to determine whether these documents should remain in this category is not required. This review is necessary only when specific circumstances require such action. (Request for this information under the Freedom of Information Act or the Privacy Act would necessitate a review of this type).

SENDING COMMENTS ON THE PROPOSED PROTECTIVE MEASURES TO NRC:

Correspondence to or from the NRC related to these enhanced security physical protection measures, not otherwise designated as Safeguards Information, will not be publicly disclosed by the NRC except as required by law.

In order to assure there is no unauthorized release of licensee-generated sensitive unclassified information related to the proposed security Protective Measures (PMs), Implementing Guidance, and Regulatory Issue Summary (RIS) Threat Conditions Table, licensees must comply with the following document marking requirements.

When providing comments on the PMs, Guidance or RIS Table, licensees shall ensure that the top of the first page of the Licensee's document and the top of each page containing the sensitive information be marked as follows: