GUIDANCE TO LICENSEES FOR THE HANDLING AND PROTECTION OF SENSITIVE UNCLASSIFIED INFORMATION AND OFFICIAL USE ONLY INFORMATION, INCLUDING PHYSICAL PROTECTION 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 security plans and other sensitive information generated in response to the Protective Measures (PMs) and associated guidance affiliated with the security Order to licensees authorized to possess certain quantities of radioactive material of concern, are sensitive information, and are to be protected from unauthorized disclosure.

Each licensee must protect this information from unauthorized disclosure. 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 needs the information to conduct business. The NRC expects this guidance to be compatible with licensees' information protection strategies.

PROTECTING LICENSEE'S PHYSICAL PROTECTION INFORMATION AND OTHER SENSITIVE UNCLASSIFIED INFORMATION

ACCESS: Dissemination of sensitive unclassified and physical-protection information by licensees must be limited to individuals that have a "need-to-know" a licensee's security information to perform their job duties, and are determined trustworthy and reliable using criteria consistent with those requirements in PM 1. Access by licensee employees, agents or contractors must include both an appropriate need-to-know as determined by the licensee, as well as an appropriate determination concerning the trustworthiness and reliability of individuals having access to the information. Employees of an organization affiliated with the licensee's company, e.g., a parent company, may be considered as employees of the licensee for access purposes. Licensee's should assure that individuals not authorized to receive such information do not overhear conversations relating to the substantive portions of the sensitive information.

Occupational Groups Considered to be Trustworthy and Reliable

Dissemination of licensee's physical protection information is limited to individuals who have an established need-to-know and who are trustworthy and reliable. Other than those individuals authorized by the licensee, members of certain occupational groups may be deemed trustworthy and reliable by virtue of their employment status. These occupational groups are:

1. An employee, agent, or contractor of the Commission, or the United States Government;
2. A member of a duly authorized committee of the Congress;
3. The Governor of a State or his designated representative;
4. A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC;
5. A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during security emergencies; or

6. A person to whom disclosure is ordered pursuant to Section 2.744(e) of Part 2 of Part 10 of the Code of Federal Regulations.
7. State Radiation Control Program Directors (and State Homeland Security Directors) or their designees.

In a generic sense, the individuals described above in (2) through (7) are considered to be trustworthy and reliable by virtue of their employment status. For non-governmental individuals in group (1) above, a determination should be made that an appropriate non-disclosure agreement exists. Discretion must be exercised in granting access to these individuals. If there is any indication that the recipient would be unwilling or unable to provide proper protection for the licensee's physical protection information they should not be authorized to receive it.

WHEN SENSITIVE UNCLASSIFIED INFORMATION IS MARKED: A U.S. Government Agency marks a document as OFFICIAL USE ONLY (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 "**Withhold from Public Disclosure in Accordance with 10 CFR 2.390.**"

MARKINGS: OUO documents are marked, by the Government Agency, 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 "**Withhold from Public Disclosure in Accordance with 10 CFR 2.390.**" Information generated by the licensee in response to the Order, Protective Measures, and associated guidance that is sent to the NRC also needs to be marked, "**Withhold from Public Disclosure in Accordance with 10 CFR 2.390**." Other licensee generated plans for the physical protection of the radioactive material covered under the Orders should be marked in such a manner to assure easy identification and to ensure proper handling.

FILES OR FOLDERS: The front and back of folders containing sensitive information should be marked 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, "**Withhold from Public Disclosure in Accordance with 10 CFR 2.390,**" or other appropriate markings indicating the category of information, should be placed at the top and bottom of only the first page of the transmitted document. In addition, the following marking should be 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: The use of Cover Sheets is a good practice for sensitive information to facilitate identification or protection of the information so that it cannot be surreptitiously or inadvertently read by individuals without the need-to-know.

REPRODUCTION: A good practice is to minimize the number of copies of documents containing, or said to contain, sensitive unclassified information 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 should be addressed to an individual authorized access to that information. Material used for packing should 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 should 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 should 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 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. U.S. or other paper mail transmission channels are preferred. When transmitting information via internet, licensees should consider encrypting sensitive unclassified information, such as physical protection information relating to your site. Licensees may use standard encryption, password, or other such features offered with computer software and with computer operating systems.

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 the sensitive information and the user is appropriately briefed on the proper security procedures while using the computer system. Individuals should 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: If a facility has an electronic access control system in place or contract guards on duty, no additional storage requirements are 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. Information stored in non-removable electronic form should be password protected. Access to the keys, combinations, passwords or other means used to secure the information needs to be limited to those persons authorized.

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 need to 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: 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.

CORRESPONDENCE TO NRC RELATED TO SECURITY ORDERS

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 physical protection information related to, or in response to, the security PMs, Implementing Guidance, Regulatory Issue Summary (RIS) Threat Conditions Table, or to any other document provided to the licensee, licensees' correspondence needs to be marked at the top of the first page of the document and the top of each page containing any information that may be considered sensitive information as follows:

"Withhold From Public Disclosure Under 10 CFR 2.390"