

**UNCLASSIFIED**

**Section 2. Specific Categories of Information**

*This section applies to specific categories of SBU or equivalent CUI used by your department or agency. Please complete a separate table for each separate category of information.*

Category Name	Official Use Only - Security-Related Information (SUNSI)	Point of Contact (name, phone, email)	Russell A. Nichols, 301-415-6874, ran2@nrc.gov
Formal Definition	<p>10 CFR 2.390(d) Information</p> <p>Information that could be useful, or could reasonably be expected to be useful to a terrorist in a potential attack that does not qualify as Safeguards Information.</p> <p>Sensitive Homeland Security Information – Department of Homeland Security (DHS)</p> <p>Licensee-submitted information that may qualify as Critical Infrastructure Information as defined by other agencies including – Critical Energy Infrastructure Information (CEII) – Federal Energy Regulation Commission (FERC), and Sensitive Security Information (SSI) – Transportation Safety Administration (TSA)</p>		
Marking	<p>NRC-Generated Documents – Mark at top and bottom of each page, “Official Use Only – Security-Related Information”</p> <p>Documents Generated by Licensees, Applicants, Contractors or Other Outside Persons/Organizations Subject to NRC Jurisdiction – Mark the top of each page, “Security-Related Information – Withhold Under 10 CFR 2.390”</p>		
Authority (law, regulation, policy, etc.) [Please enclose copies of reference documents if possible]	<p>10 CFR 2.390</p> <p>“NRC Policy for Marking, Handling and Protecting Sensitive Unclassified Non-Safeguards Information,” October 26, 2005</p> <p>NRC Management Directive 12.6, “NRC Sensitive Unclassified Information Security Program,” June 2, 1998 (Revised: December 20, 1999)</p>		
Is this category of information used only by specific elements within your department, or does it apply agency-wide? Is it recognized broadly across the U.S. Government?	<p>The use of the designation “Official Use Only – Security-Related Information” applies agency-wide to the NRC. It is not recognized broadly across the U. S. Government.</p>		
Who is authorized to apply this designation?	<p>The originator, supervisor or principal recipient.</p>		
Who is authorized to remove the designation? What criteria are used?	<p>The originating office or office primarily responsible for the information. Currently, there is no documented criteria for removal of this SBU designation.</p>		
Are there provisions for automatic removal of the designation after a specified time?	<p>No. However, the information would be reviewed for removal of the designation upon receipt of a Freedom of Information Act request for the information.</p>		
Are there any special restrictions on access to	<p>Yes. Access is restricted to NRC personnel or NRC contractor employees who need to know the information to perform their official</p>		

**UNCLASSIFIED**

UNCLASSIFIED

Section 2. Specific Categories of Information	
this category of information, by agencies or individuals?	duties.
Are there any special provisions governing access to this information by State, local, or tribal governments or private sector entities?	Yes. A “need-to-know” determination must be made before access is granted to State, local, or tribal governments or private sector entities.
Describe any procedures for processing, storing, tracking, or disseminating this category of SBU or equivalent CUI, including any special requirements that apply to automated information systems.	<p>Official Use Only (OUO)-Security-Related Information may be processed on the NRC local area network (LAN) and other systems accredited under NRC Management Directive 12.5, “NRC Automated Security Program.”</p> <p>On NRC Electronic Systems: OUO-Security-Related Information may be stored on NRC computer systems that have a security plan and accreditation approval.</p> <p>Storage Inside the NRC (Headquarters and Regional Offices): OUO-Security-Related Information may be stored openly or in a non-locking container within areas where there is supplemental security, including electronic access controls (keycard) and/or guards on duty. If management determines additional protection is needed, the information should be stored in key locked file cabinets or equivalent storage containers.</p> <p>Storage Outside the NRC (Resident Inspector Sites): When supplemental security such as electronic access is either unavailable or guards are not on duty, OUO-Security-Related Information may be stored in key locked desks or other key locked containers.</p> <p>There is no mechanism for tracking OUO-Security-Related Information at the NRC.</p> <p>There is no restriction on reproduction unless stated on the document; reproduction is limited to the number of copies needed for official use. Copies must clearly show the original markings.</p> <p>OUO-Security-Related Information may be entered into the ADAMS main library and must be profiled as Non-Publicly Available and Sensitive. Access rights are assigned to user groups with a need to access the information to perform their official duties.</p> <p>Special Requirements for TSA-Generated SSI: Always store SSI in a locked drawer, cabinet or behind a locked door when not in the physical possession of an authorized person with a need-to-know.</p>
Describe procedures for marking this category of SBU. Is information marked at the document or paragraph level?	The document is marked “Official Use Only – Security-Related Information” with a header and footer. Paragraph markings are not required within the document.

UNCLASSIFIED

## Section 2. Specific Categories of Information

Describe any training or guidance given to department or agency employees regarding marking, storing, or handling of this category of SBU.

SUNSI training is an annual requirement at the NRC. Four training sessions were held at the Headquarters NRC in November, December 2005, and January 2006. One of the training sessions was video recorded and is available from the NRC Professional Development Center (PDC). The PDC is making CD's of the training for dissemination, and the training will be available in electronic form on the PDC Website. An on-line tutorial computer-based training module is being planned but has not yet been developed.