Chapter 13 Revision History as of 5/9/19:

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Date</th>
<th>Changed</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destruction</td>
<td>8/10/2016</td>
<td>-</td>
<td>Add Hours and locations for burn bag drop-offs at FORS and GTN</td>
</tr>
<tr>
<td>Controlled Unclassified Information (CUI)</td>
<td>4/13/2017</td>
<td>Pg. 13-1, second paragraph, use of the term CUI</td>
<td>Changed to read: “CUI also describes information identified and safeguarded under Executive Order 13556, CUI and its implementing directive 32 CFR 2002. These mandate a government wide uniform program to identify and protect sensitive but unclassified information. Until DOE issues an order implementing CUI, DOE personnel must continue to follow the regulations and directives for UCNI and OUO information.”</td>
</tr>
<tr>
<td>Transmission of UCNI</td>
<td>5/9/2019</td>
<td>Added – packaging requirements.</td>
<td>Added: The document or material must be packaged to conceal the presence of the UCNI from someone who is not authorized access.</td>
</tr>
<tr>
<td>Transmission of OUO</td>
<td>5/9/2019</td>
<td>The option to encrypt OUO material transmitted over DOE IT systems</td>
<td>Added: When sending OUO over DOE IT systems, EITS policy requires that all DOE employees and contractors ensure the information is encrypted. This pertains to all CUI data.</td>
</tr>
<tr>
<td>Headquarters Implantation Procedures</td>
<td>5/9/2019</td>
<td>This section has been extensively rewritten</td>
<td>Added: Additional access requirements for UCNI and OUO material (pages 13-3 &amp; 13-4).</td>
</tr>
</tbody>
</table>
Chapter 13
Controlled Unclassified Information

This chapter describes the security procedures adopted by DOE HQ to implement the requirements of the following DOE regulations and directives:

10 CFR Part 1017, Identification and Protection of Unclassified Controlled Nuclear Information

DOE Order 471.1B, Identification and Protection of Unclassified Controlled Nuclear Information

DOE Order 471.3, Chg 1, Identifying and Protecting Official Use Only Information

DOE Manual 471.3-1, Chg 1, Manual for Identifying and Protecting Official Use Only Information

Within DOE, Controlled Unclassified Information (CUI) refers to unclassified information identified and marked as sensitive. CUI also describes information identified and safeguarded under Executive Order 13556, CUI and its implementing directive 32 CFR 2002. These mandate a government-wide uniform program to identify and protect sensitive but unclassified information. However, until DOE issues an order implementing E.O. 13556, DOE personnel must continue to follow the regulations and directives for UCNI and OUO information.

Within DOE, CUI includes:

- Unclassified Controlled Nuclear Information (UCNI)
- OUO, which encompasses Personally Identifiable Information (PII), Export Controlled Information (ECI), and other unclassified sensitive information not governed by specific directives

Note: Confidential Foreign Government Information-Modified Handling Authorized (C/FGI-MOD) is classified under Executive Order 13526 and does not fall under this section (see Section 504, Foreign Government Information).
Transmission

UCNI:

A document containing UCNI may be transmitted by (1) U.S. First Class, Express, Certified, or Registered mail; (2) any other means approved for transmitting a classified document; (3) an authorized individual as long as physical control of the package is maintained; or (4) mail services internal to the facility. The document or material must be packaged to conceal the presence of the UCNI from someone who is not authorized access. A single, opaque envelope or wrapping is sufficient for this purpose. The address of the recipient and the sender must be indicated on the outside of the envelope or wrapping along with the words “TO BE OPENED BY ADDRESSEE ONLY.”

Encryption must be used when transmitting UCNI over a telecommunications circuit (e.g., telephone, facsimile, radio, e-mail, Internet). FIPS 140-2 is the standard that must be used when transmitting CUI via electronic means.

OUO:

A document containing OUO may be transmitted by (1) First Class, Express, Certified, or Registered mail as well as by any commercial carrier; (2) a person authorized access to the OUO so long as the person can control access to the document being transported; or (3) mail services internal to the facility. For documents sent outside a facility, the document must be packaged in a sealed, opaque envelope with the recipient’s address, a return address, and the words “TO BE OPENED BY ADDRESSEE ONLY” on the front. For documents sent within a facility, the document must be packaged in a sealed, opaque envelope with the words “TO BE OPENED BY ADDRESSEE ONLY” on the front, but only the recipient’s address is required. When sending OUO over DOE IT systems, EITS policy requires that all DOE employees and contractors ensure the information is encrypted. This pertains to all CUI data.

Destruction

Documents containing CUI must be destroyed by shredding. CUI must not be put in the recycle bins. A document containing CUI may be destroyed using a cross-cut shredder producing particles no larger than ¼ inch x 2 inches. Shredders meeting this requirement are available in the self-service supply stores.

Bulk paper, plastic, and metal waste (not including hard drives – see note below) containing CUI must be sorted and placed in plain brown paper bags and delivered to the Burn Bag Rooms (Forrestal GI-007 and Germantown R-002) for destruction. The name, routing symbol, telephone number, and room number of the person responsible for the burn bag and the type of material contained within (i.e., paper, plastic, or metal) must be clearly marked on each bag for identification. The weight limit for each bag is 10 pounds for bags generated at Forrestal and 15 pounds for those generated at Germantown.
The difference in weight limitation results from transportation and handling requirements. The top of the bags should be folded over at least once and stapled shut every 2 inches. Burn bags must be protected as CUI until they are destroyed. Personally owned, non-official waste material including food waste products are not to be included in the Burn Bags. Failure to comply with destruction preparation procedures may result in the issuance of a security infraction.

Note: Unclassified hard drives MAY NOT be delivered to a Burn Bag Room for destruction. Call (301) 903-2500 to arrange for unclassified hard drives to be picked-up and stored by IM until arrangements are made for the hard drives to be destroyed by a qualified outside vendor.)

Note: Paper clips, heavy duty staples, and metal or plastic fasteners must be removed from all paper documents and waste.

Documents and material containing CUI may also be destroyed by methods approved for the destruction of classified matter.

Burn bags may be delivered to the following collection points during the times listed:

- Forrestal Building – Room GI-007 between 3:00 p.m. and 4:00 p.m., Mondays, Wednesdays and Fridays.
- Germantown Building – Room R-002 between 9:30 a.m. and 10:30 a.m., Mondays, Wednesdays and Fridays.

**HQ Implementation Procedures**

Complete requirements for access, identification and protection of UCNI and OUO are contained in the respective DOE regulations and directives listed above. The following points are included here for emphasis:

While a clearance is not required for access to UCNI or OUO, access is still controlled. Subpart D of 10 CFR Part 1017 contains defined requirements for access to UCNI. Authorization for routine access depends on whether the individual is a U.S. citizen or not. The authorization for routine access is more limited for individuals who are non-U.S. citizens. However, any employee or contractor of the Department of Energy, to include non-U.S. citizens, is authorized for routine access to UCNI if the individual has a “need to know” in order to perform official duties. In some instances, individuals who are not authorized for routine access may be granted limited access if a written request is submitted under 10 CFR 1017.21. Note that violations of the UCNI access and protection requirements in Subpart D can result in severe penalties.

Access to OUO may be granted to a person who needs the information to perform a DOE-authorized function (i.e., “need to know”), as determined by the person who has authorized possession, knowledge, or control of the information. Individuals who perform authorized DOE functions may include Federal, state or local government employees; the private sector; and foreign nationals, as long as there is a valid need for access. It is important to note, however, that some OUO (e.g., Export Controlled Information, Source Selection Information) has additional access restriction.
If a document is in a classified subject area, it must be reviewed by the appropriate classification official identified in DOE O 475.2B. If the document does not contain classified, but contains OUO or UCNI the document must be marked as specified in regulatory and directive requirements.

Anyone who originates or possesses a document or material that he or she thinks may contain UCNI must have it reviewed by an UCNI Reviewing Official before it is (1) finalized, (2) sent outside of the originating organization, or (3) filed. If the originator or possessor must send the document outside of his or her organization for the review, he or she must mark the front of the document with “Protect as UCNI Pending Review” and must transmit the document in accordance with the requirements in 10 CFR 1017.27.

Any Federal or contractor employee may determine that an unclassified document contains OUO information. Such determinations must be limited to documents or material that were originated within, produced for, or are otherwise under the control of his or her office. Before making an OUO determination, the employee must be familiar with the OUO directives, including the marking and protection requirements. Information identified as OUO in Office of Classification issued guidance or in guidance from the employee’s program office must be marked OUO. If the information is not covered by guidance, the employee may determines whether the information is OUO under DOE M 471.3-1, Chg. 1.

Documents containing UCNI or OUO must not be posted on websites available to the public. For requirements concerning posting UCNI and OUO on internal DOE websites, contact the Office of the Chief Information Officer (IM-622).

Documents and material containing UCNI or OUO must be reviewed in accordance with program office policies prior to public release (e.g., posted on a website), and the appropriate personnel must remove the UCNI and OUO.

Documents that contain OUO or UCNI do not have additional accountability requirements.

The originating agency establishes protection requirements for other-agency CUI – for example, Sensitive But Unclassified (SBU), For Official Use Only (FOUO), and Administratively Controlled Information (ACI). In most cases, when other-agency protection requirements cannot be determined, documents bearing these markings should be protected within DOE HQ as OUO. However, there are several exceptions. These include, but are not limited to Nuclear Regulatory Commission Safeguards Information (SGI) and the Department of Homeland Security Sensitive Security Information (SSI). If unsure how to handle other-agency CUI, contact the person who transmitted the information for clarification and direction.

**Points of Contact**

For information about CUI, call (301) 903-4861 or (301) 903-7567.
Additional Information

The Office of Classification’s website has a page with information concerning OUO (OUO Information website) and another on UCNI (UCNI Information Website). These pages contain information, resources, and links to the DOE regulation and directives concerning CUI.

The DOE CMPC Marking Resource has additional information concerning marking documents containing CUI. To access the DOE CMPC Marking Resource go to: DOE Marking Resource