Chapter 13 Revision History: Revisions by date (Newest to oldest):

January 29, 2020:

- Revised the CUI Subsection: Changed the term CUI to reflect only information under E.O. 13556 and 32 CFR 2002, added SAO for CUI, addressed marking burn bags containing OUO and UCNI

May 9, 2019:

- Revised the Transmission of UCNI Subsection: Added packaging requirements. "The document or material must be packaged to conceal the presence of the UCNI from someone who is not authorized access.
- Revised the Transmission of OUO Subsection: Changed the option to encrypt OUO material transmitted over DOE IT systems. 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."
- Revised pages 13-2 and 13-4 to provide additional access requirements of UCNI and OUO material.

Chapter 13
Controlled Unclassified Information

Executive Order 13556, Controlled Unclassified Information (CUI), and its implementing directive 32 CFR 2002 mandate a government wide uniform program to identify and protect sensitive but unclassified information. The Chief Information Officer is the Senior Agency Official for CUI responsible for developing CUI policy. Until an order implementing Executive Order (E.O.) 13556 is issued, DOE personnel must continue to follow the regulations and directives for UCNI and OUO information. This section addresses current requirements for UCNI and OUO.

Within the Department of Energy (DOE), CUI currently refers to information designated as:

1. Official Use Only (OUO) (including Export Control Information [ECI], Personally Identifiable Information [PII], and other information specifically designated as requiring protection e.g., sensitive unclassified Cooperative Research and Development Agreements [CRADA] information),
2. Unclassified Controlled Nuclear Information (UCNI), and
3. Unclassified Naval Nuclear Propulsion Information (U-NNPI).

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).

Currently, there is no DOE directive implementing EO 13556. The DOE Chief Information Officer is the Senior Agency Official responsible for developing CUI policy under E.O. 13556. Until specific CUI DOE directives are issued, information designated as OUO and UCNI will continue to be managed in accordance with the following directives and regulations:

a. DOE Policy (P) 205.1, *Departmental Cyber Security Management Polic*y,
b. DOE Order (O) 205.1C, *Department of Energy Cyber Security Program,*
c. DOE O 206.1, Chg 1, *Department of Energy Privacy Program,*
d. 10 C.F.R. 1017, *Identification and Protection of Unclassified Controlled Nuclear Information,*
e. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information,*
f. DOE O 471.3, AdmChg 1, *Identifying and Protecting Official Use Only Information, and*
g. DOE Manual (M) 471.3-1, AdmChg 1, *Manual for Identifying and Protecting Official Use Only 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). Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2) is the standard that must be used when transmitting UCNI 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 of 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 the DOE information technology (IT) system, Energy IT Services (EITS) policy requires that all DOE Federal employees and contractors ensure that the information is encrypted. This pertains to all CUI data.

Destruction

Documents containing UCNI and OUO must be destroyed by shredding or by a method approved for classified matter. UCNI and OUO must not be put in the recycle bins. At DOE Headquarters, a cross-cut shredder producing particles no larger than ¼ inch x 2 inches (available in the self-service supply stores) must be used when shredding a document containing UCNI and OUO.

Bulk paper, plastic, and metal waste (not including hard drives – see note below) containing UCNI and OUO must be placed in plain brown paper bags and delivered to the Burn Bag Rooms (Forrestal GI-007 and Germantown R-002) for destruction. Paper clips, heavy duty

staples, and metal or plastic fasteners must be removed from all paper documents and waste. Each plain brown bag must be marked with the appropriate acronym to indicate the sensitivity of the matter. If the plain brown bag contains UCNI, or UCNI and OUO, it must be marked with "UCNI." If it contains only OUO, it must be marked with "OUO." 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 also 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 top of the bags should be folded over at least once and stapled shut every 2 inches. Burn bags must be protected as UCNI or OUO until they are destroyed. Personally owned, non-official waste material including food waste products must not to be included in Burn Bags. Failure to comply with destruction preparation procedures may result in the issuance of a security infraction.

Unclassified hard drives MUST 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 the Office of Chief Information Officer (IM) until arrangements are made for the hard drives to be destroyed by a qualified outside vendor.

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.

Complete requirements concerning the identification and protection of UCNI and OUO are contained in the directives and regulation cited in the references. The following sections are not comprehensive and are provided for emphasis.

Access to UCNI and OUO

A clearance is not required for access to UCNI or OUO.

Any Government Federal or contractor employee with a need to know may have routine access to UCNI or OUO. Any employee or representative of a State, local, or tribal government with a need to know may also have routine access to UCNI. Refer to Subpart D of 10 CFR Part 1017.21 for additional information on who can have routine access to UCNI, and procedures for allow individuals without routine access to request limited access. Note that violations of the UCNI access and protection requirements 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 restrictions.

Review Requirements for UCNI and OUO

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 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 should 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 and material containing UCNI or OUO must be reviewed in accordance with program office policies prior to public release and the appropriate personnel must remove the UCNI and OUO.

Other Handling Requirements for UCNI and OUO

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, Service Desk and Application Support Office (IM-622).

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 UCNI or OUO, call (301) 903-4861 or (301) 903-7567.