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

January 22, 2024:

- Updated Controlled Unclassified Information (CUI) to reflect DOE O 417.7, including addressing Unclassified Controlled Nuclear Information (UCNI) as CUI Specified and Official Use Only (OUO) as legacy information.

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. On February 3, 2022, DOE Order (O) 471.7, *Controlled Unclassified Information,* was issued to implement the DOE CUI Program. At that time, OUO was rescinded. The Chief Information Officer is the Senior Agency Official for CUI and the office responsible for DOE-wide implementation is IM-41. Under DOE O 471.7, the DOE CUI Program is further implemented by Departmental Element Designated CUI Officials.

This chapter provides basic information on CUI and Unclassified Controlled Nuclear Information (UCNI). UCNI is certain unclassified design and security information concerning nuclear facilities, material, and weapons that are controlled under the Atomic Energy Act. Because of the sensitivity of the information, very specific requirements for UCNI are in Title 10 Code of Federal Regulations Part 1017 and DOE O 471.1B. Under CUI, information with specific requirements in law, regulation, and Government-wide policy (LRGWP) are CUI Specified and the requirements under LRGWP take precedence. Therefore, UCNI must continue to be reviewed, identified, marked, and protected as required under these policies and must not be marked under CUI policies (e.g., CUI//SP-UCNI). No other CUI markings are required on documents containing UCNI. However, if the UCNI is decontrolled or removed, the document must be reviewed for CUI and appropriately marked if it contains CUI. For clarification, each section addresses CUI and UCNI separately. **Note that complete requirements concerning the identification and protection of UCNI are contained in the regulation and directive cited in the references. The following sections are not comprehensive and are provided for emphasis.**

The following directives and regulations apply to CUI:

- **a.** DOE Policy (P) 205.1, *Departmental Cyber Security Management Polic*y,
- **b.** DOE Order (O) 471.7, *Controlled Unclassified Information,*
- **c.** DOE O 206.1, Chg 1, *Department of Energy Privacy Program, or current version,*
- **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.*

Access

CUI:

According to 32 CFR 2002.16, authorized holders must meet four conditions to permit access to or dissemination of CUI:

1. Follow laws, regulations, or Government-wide policies that established the CUI category or subcategory.
2. Access furthers a lawful Government purpose.
3. Access isn't restricted by an authorized limited dissemination control established by the CUI Executive Agent (EA).
4. Is not otherwise prohibited by law.

UCNI:

A clearance is not required for access to UCNI.

Any Government Federal or contractor employee with a need to know may have routine access to UCNI. Any employee or representative of a State, local, or tribal government with a need to know may also have routine access to UCNI. If a person is not covered under this information, refer to Subpart D of 10 CFR Part 1017.21 for additional information on who may have routine access to UCNI, and procedures for allowing individuals without routine access to request limited access. Note that violations of the UCNI access and protection requirements can result in severe penalties.

Review Requirements

UCNI:

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.

Documents and material containing UCNI must be reviewed in accordance with program office policies prior to public release and authorized personnel must remove the UCNI.

Transmission

CUI:

A document containing CUI 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 CUI 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 CUI 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. When sending CUI via email to accounts outside of Federal IT systems the CUI must be in an attachment and protected by encryption or password protection unless the authorized holder assesses that the immediate mission and business needs outweigh any risk of sending the email without encryption or password protection. In such situations, authorized holders may be required by their supervisor to provide a written statement regarding their determination. The password must be transmitted separately from the email attachment containing CUI (e.g., by phone or text).

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.

Destruction

CUI:

The CUI regulation requires that agencies destroy CUI "in a manner that makes it unreadable, indecipherable, and irrecoverable," (32 CFR 2002.14(f)(2)). It also prescribes National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Revision l: Guidelines for Media Sanitization (December 2014) (NIST SP 800-88, rev 1) destruction methods, or any destruction method approved for Classified National Security Information (32 CFR 2001.47), unless the CUI category's authority mandates other destruction methods (CUI Specified

Crosscut shredders purchased prior to the issuance of DOE O 471.7, and not identified on the NSA EPL, may continue to be used for the destruction of CUI paper matter and non-paper products, excluding microfilm. However, these shredders must be replaced once they become unserviceable or after 5 years after the effective date of the order.

Agencies must also use any destruction method specifically required by law, regulation, or Government-wide policy for CUI Specified categories. ISOO clarifies certain aspects of the requirements for destroying paper CUI. NIST SP 800-88, rev 1 describes authorized methods for destroying other media types that contain CUI.

For the single-step destruction method agencies must:

a. Use cross-cut shredders that produce 1 mm x 5 mm (0.04 in x 0.2 in.) particles (or smaller); or
b. Pulverize/disintegrate paper using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. For more information see: CUI Notice 2019-02: Destroying Controlled Unclassified Information (CUI) in Paper Form (archives.gov).

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

UCNI:

Documents containing UCNI must be destroyed by shredding or by a method approved for classified matter. UCNI 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 must be used when shredding a

document containing UCNI. UCNI may also be placed in plain brown paper bags and delivered to the Burn Bag Rooms (Forrestal GI-007 and Germantown R-002) for destruction. If the plain brown bag contains UCNI, it must be marked with "UCNI" regardless of any other markings. See CUI for additional information on the use of burn bags.

OUO

OUO is no longer authorized as a marking for controlled unclassified information. Legacy information marked OUO, or other expired marking formats are waivered for remarking, unless the material is re-used to create a new document, or the material is sent outside of the Department. If information is re-used or sent outside of the Department, it must be marked with the correct CUI category marking.

Other Handling Requirements

CUI: Handling of Paper CUI documents

Printed CUI documents must be kept under direct control of an authorized holder, utilize a CUI coversheet, and be protected by at least one physical barrier such as a locked cabinet or door during storage.

- Do not send CUI to the printer unless you are able to be at the printer when it prints.
- Do not let CUI documents sit on the printer where unauthorized people can have access to the information.
- If possible, use a printer that requires you to enter a code before printing.
- Ensure proper marking, including:
    - CUI documents must have the CUI marking on each printed page.
    - A CUI cover sheet must be used in lieu of banner markings when it is impractical to individually mark every page due to its quantity, legacy status, or the nature of the information.
    - The CUI cover sheet (Standard Form 901) is available through the GSA forms library or can be downloaded and printed from the CUI Registry.

Mailing CUI materials

- Address the envelope/package to a specific recipient (not to an office or organization).
- Do not put CUI markings on the outside of the envelope/package.
- Use automated tracking on the package to ensure it was delivered to the correct recipient.
- You may use the following methods to transport CUI:
    - The U.S. Postal Service (USPS)
    - Any commercial delivery service (FedEx, UPS)
    - Interoffice mail delivery
    - Interagency mail delivery

CUI: Handling of Electronic CUI documents

- CUI may only be digitally stored in an authorized IT system/application that is:
    - configured at not less than the Moderate Confidentiality impact value.
    - has limited access based on need.
- CUI being emailed outside the DOE network must be sent as a FIPS-compliant encrypted attachment.
- When sending CUI outside a DOE network, CUI must be sent as an encrypted attachment to their email address. The body of the email must not contain any CUI but must include the applicable CUI markings at the top of the email message. See this CUI Registry page for more details on email markings.

UCNI:

A person with access must maintain physical control over any document or material that contains UCNI to prevent unauthorized access. Measures must be taken to ensure documents cannot be accessed by unauthorized persons and UCNI may not be seen or overheard by unauthorized persons.

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

Documents that contain UCNI do not have additional accountability requirements.

Additional Information

CUI:

Additional information, including a brochure and training for persons with access to CUI is available to DOE personnel on PowerPedia at Controlled Unclassified Information - Powerpedia (energy.gov)

UCNI:

Additional information, including a brochure and training for persons with access to UCNI is available on PowerPedia at Unclassified controlled nuclear information - Powerpedia (energy.gov).

Points of Contact

For information about UCNI contact the Classification Outreach Program at (301) 903-7567 or outreach@hq.doe.gov.

For information on CUI, email doecui@hq.doe.gov or your Departmental Element Designated CUI Official.