Pantex | Managed and Operated by PANTEXAS DETERRENCE

Identification and Protection of UCNI/CUI for Vendors and Subcontractors

Heather Caudill

Heather.Caudill@Pantex.Doe.Gov

Pantex Classification Office

This document has been reviewed by a DC/RO and has been determined to be UNCLASSIFIED, not UCNI, and contains no CUI based on current classification guidance. This review does not constitute a review for CUI outside of classification guidance and does not constitute clearance for Public Release.

Name: Heather Caudill
Date: 2/6/2025
Pantex eDC/RO ID: 890239

Controlled Unclassified Information (CUI) and Unclassified Controlled Nuclear Information (UCNI)

- The U.S. Department of Energy (DOE) has established the following orders to guide the protection of CUI/UCNI:
  - DOE O 471.7, *Controlled Unclassified Information* (Feb 2022), standardizes CUI across the DOE complex.
    - Former Official Use Only (OUO) order and manual (DOE O 471.3 and DOE M 471.3-1) are canceled/superseded {OUO designation is now considered legacy}.
  - DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, remains active and compliments existing UCNI law (10 CFR 1017).
- DOE Office of Classification has directed all contractor and federal employees to continue to identify and protect UCNI in accordance with already established DOE orders and federal regulations.

Some Types of Protected Information

- **Controlled Unclassified Information (CUI):** Unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy. Includes two categories (or types): Basic and Specified

- **Unclassified Controlled Nuclear Information (UCNI):** Unclassified but sensitive information concerning nuclear material, weapons, design of production facilities, utilization of weapons or components, security measures for the protection of facilities, materials, and information. This information is prohibited from unauthorized dissemination under Section 148 of the Atomic Energy Act, revised. Reference 10 CFR 1017 and Atomic Energy Act of 1954, revised.

- **Export Control Information (EXPT):** Includes scientific and technical information or equipment containing technical data as defined and controlled by the International Traffic in Arms Regulations (ITAR), Export Administration Regulations, Nuclear Nonproliferation Act of 1978, and the Atomic Energy Act of 1954, as amended. Technology and products are controlled to prevent unauthorized release to foreign countries, organizations, or individuals

UCNI/CUI Orders, Regulations, and Policies

Applicable Law and DOE Regulatory Requirements

10 CFR 1017 DOE O 471.1B	*Identification and Protection of Unclassified Controlled Nuclear Information*
DOE O 471.7 32 CFR Part 2002	*Controlled Unclassified Information*

Applicable Procedures and Policies

MNL-352366	*Export Compliance Procedure*
MNL-352350	*Identification and Protection of Unclassified Controlled Nuclear Information and Controlled Unclassified Information*
PX-6923	*UCNI/CUI Protection Requirements for Pantex Suppliers*

Access to UCNI

- Does not require a clearance
- Must be a citizen of the United States (foreign national access limitations exist)
  - Legal permanent resident (LPR) or work visa does not constitute access or citizenship.
    - For Export Controlled Information ONLY- An LPR is considered a U.S. citizen and held to the same federal export laws and regulations.
  - Maintain proof of citizenship of individual and make available to Pantex when requested.
  - Acceptable documents for proof of citizenship include the following:
    - Birth certificate [certified copy with official seal issued by government/municipality (not issued by hospital)]
    - *Certificate of Naturalization* [Immigration and Naturalization Services (INS) Form N-550 or N-570]
    - *Certificate of U.S. Citizenship* (INS Form N-560 or N-561)
    - *Report of Birth Abroad of a Citizen of the United States of America* (Form FS-240)
    - U.S. passport (active) with picture that looks like the individual

Access to UCNI and CUI

- All employees with access to UCNI/CUI must be briefed on protection requirements prior to being provided access (i.e., completion of this briefing followed by signed acknowledgment agreement)
- **UCNI/CUI access is limited to need-to-know**
  - Need-to-know means an individual requires access to specific information to perform official work responsibilities
    - Curiosity is not a need-to-know. Supervision of an individual is not a need-to-know.
  - Need-to-know is granted by the authorized holder of the information or material.

Access to UCNI and CUI

Access must be controlled

- While in use, the person granted access to UCNI or CUI must maintain physical control over any UCNI/CUI to protect it from unauthorized access.
- When not in use, documents must be stored to preclude unauthorized disclosure. This information must be stored in locked receptacles (e.g., file cabinets, desk drawers) under key or combination control with only individuals with need-to-know having access to keys or combinations and in a manner that prevents inadvertent access by an unauthorized individuals.
- Handling or processing:
  - Perform in a facility’s closed, unobservable office or area – or in such a manner as to preclude unauthorized access/viewing
  - MUST NOT be in areas susceptible to casual viewing (i.e., public areas)
- UCNI/CUI work areas and computers that are used for the processing of UCNI/CUI must have the means to protect the information from unauthorized viewing and be configured to resist unauthorized entry (i.e., access controls).
- While in transit, documents must be packaged to conceal information and adhere to requirements as defined by law, regulation, or government-wide policy. Refer to DOE O 471.7 and PX-6923 for more details.

The less people you have handling UCNI/CUI the better.

Lower-Tier Subcontractors

- Subcontractor may issue UCNI/CUI documents to lower tiers after the buyer's approval.

- Lower-tier subcontractors are held to the same requirements prior to receiving UCNI/CUI:
  - Citizenship
  - Protection measures
  - Training
  - Need-to-know or access required to perform official/government-authorized duties

- SUBCONTRACTOR is responsible to ensure any lower-tier subcontractors meet any re-training and re-certification requirements.

Processing UCNI/CUI on Computers

- Computer requires certification by Pantex Cybersecurity prior to use
  - If vendor computer system, certification to NIST 800-171 is required
  - Certification includes all protected information up to and including UCNI
- Subcontractors may obtain government-furnished equipment (GFE) (i.e., laptops, etc) in accordance with a contract, to facilitate processing of UCNI/CUI and other sensitive information during execution of their contract.
- Vendor computers may be stand-alone with no network (air-gapped) or attached to stand-alone network (air-gapped network). **Must be certified by Cybersecurity before processing UCNI/CUI.** Those who have access to the stand-alone/network must meet access and training requirements.
- All storage media (e.g., hard drive, CDs, DVDs, etc.) must be encrypted, removable, and able to be surrendered upon termination of the contract. Media (including back-up media) must be provided to Cybersecurity at completion of task or contract. Media must be marked according to instruction.

NOTE: Request for computer certification comes after the award of contract.

Processing UCNI/CUI on Computers (cont.)

- Operating system must meet requirements of Cybersecurity. Exceptions require special handling and may not be considered.

- Peripherals should not contain hard drives (printers, plotters, etc.). If peripherals contain hard drives, the media must be encrypted and will be provided to Cybersecurity at the end of the performance period.

- Media must be encrypted using published National Institute of Standards and Technology Federal Information Processing Standard (FIPS) or higher certified encryption software approved by Cybersecurity.

- **Prohibited:** Attachment to or use of corporate, company, or public networks or personal e-mail to process UCNI/CUI is **prohibited** unless approved and documented by Cybersecurity. UCNI/CUI placed on an unapproved system is an Incident Of Security Concern (IOSC) and may result in fines or contract repercussions.

- **Prohibited:** Wireless capabilities are **prohibited** unless Cybersecurity-directed FIPS standards are employed and permission through the Telecommunications Proposal process is granted.

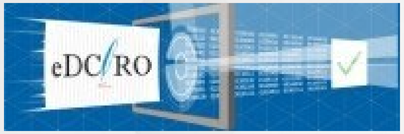
Processing UCNI / CUI on Computers

Computer or other equipment processing UCNI/CUI

- Passwords must conform to DOE requirements and be provided by Cybersecurity.
- Use of PDAs, PC tablets, smartphones, etc., for processing information require special handling and approval through the Telecommunications Proposal process. Permission may not be granted.
- Only authorized personnel may have access to computer(s) when processing UCNI/CUI. Computer(s) may be accessed by others when not being used to process UCNI/CUI and requisite media and information is removed and secured.
- **Prohibited:** Use of cell phone camera capability, built-in recording capability, and Bluetooth during the handling, processing, and/or discussing of UCNI/CUI
- If a subcontractor is supplied GFE (often referred to as a GFE laptop), at no time can any UCNI be moved from the GFE laptop to a corporate network. UCNI may only be moved from a GFE laptop to an air-gapped system that has been certified and accredited by the Pantex Cybersecurity POC and back to the GFE laptop if necessary using an encrypted "IronKey" USB storage thumb-drive or other approved process.

NOTE: Use of Wi-Fi hotspots on Pantex property is prohibited without express written approval from Cybersecurity.

Marking UCNI Documents



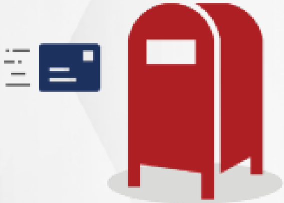
- **Marking of UCNI documents pending classification review**
  - Documents generated from a certified UCNI-approved computer require protection at the highest level of certification (i.e., UCNI) pending classification review.
  - Only a derivative classifier/UCNI-reviewing official (DC/RO) can make a determination of the document's sensitivity. Contact your subcontract technical representative (STR) if a document is identified as needing to be reviewed.
  - However, if your organization will be generating and processing a large quantity of UCNI, it's highly recommended that your organization has at least one DOE-trained DC/RO within the organization. Details on how to become a DC/RO can be obtained through the Pantex Classification Office.
  - Hard-copy documents from UCNI-approved computers should be protected as UCNI pending classification review. This will be accomplished by having a separate piece of paper marked PROTECT AS UCNI PENDING REVIEW as the first page of text for the UCNI documents with the UCNI coversheet on top.
  - Electronic documents generated using UCNI-approved computers MUST be protected as UCNI if the document is in draft until a DC/RO has made a determination. Final documents in electronic format must be marked UCNI if so determined by a DC/RO.

Transmitting UCNI/CUI

- Telephone
  - DO NOT discuss
    - UCNI over telephone. Secure phone (OMNI or STE) must be used.
    - CUI over VOIP, cordless, or cellular telephones.
- Facsimile
  - DO NOT fax UCNI.
  - Faxing is permitted for CUI with receipt confirmation by receiving individual with need-to -know access. This is done via phone call notification preceding the fax.

  DO NOT e-mail
    - UCNI without approved encryption and certification.
    - UCNI to computers that have not been certified for use.
    - When transmitting CUI, encrypt. If encryption is not available, files must be, at minimum, password protected. Contact the Pantex Classification Office for more information and advisories prior to transmission.
  - DO NOT use file services (e.g., Dropbox), social networking sites (e.g., Twitter, Facebook, etc.), or other non-approved methods for transmitting government-owned information.

Transmitting UCNI/CUI (cont.)



- **Mailing**
  - Mail by USPS Express, Registered, Certified Mail, or First Class or commercial carrier (e.g., FedEx, UPS, etc.) with signature service.
  - When mailing, place documents or media in sealed, opaque, envelope externally marked **To Be Opened By Addressee Only.** Identify specific authorized individual(s).

- **Transportation Limitations**
  - <u>DO NOT</u> place in checked baggage or gate baggage when traveling by commercial carrier (e.g., air, rail, etc.). Use briefcase or mail.
    - When hand carrying, package and seal the information and maintain positive control over documents and media.
  - <u>DO NOT</u> expose documents in public environment (e.g., restaurants, aircraft, airports, lobbies, etc.)

Refer to 10 CFR 1017 and/or DOE O 471.7 for more details on mailing UCNI or CUI

Reproducing UCNI / CUI

- **Reproduction**
  - Reproduction of UCNI/CUI is allowed on approved devices only.
  - If authorized, keep number of copies reproduced limited to the minimal amount required for the task.

DO NOT

- Dispose of errors in the trash. Be sure to destroy using an approved destruction device, methods, or return to the STR for disposal.
- Use commercial copy centers or copy services.

NOTE: During the bidding process, notify the subcontract administrator if additional copies are needed. Reproduction using company-owned equipment that has not been pre-approved is prohibited.

Destroying UCNI/CUI

Destruction

- Place UCNI/CUI in a Pantex-approved Dissemination Box (coordinate with STR)
- Follow “Protect as UCNI/CUI” procedures (i.e. locked room, or cabinet) until given to STR for proper destruction (Preferred)

- **DO NOT use a commercial shred service.**

At end of task or contract

- Notify the Procurement authority (buyer) or STR that paper material has been placed in dissemination boxes or has been returned to Pantex for further disposition.

Briefing Requirements

- Each member of your team (including lower-tier subs and vendors):
  - Must review this briefing if they will be handling UCNI/CUI.
  - Must review PX-6923, UCNI/CUI Protection Requirements for Pantex Supplier
  - Maintain a copy of briefing record, PX-6668(acknowledgment form).
  - Provide a copy of the PX-6668(via email, fax, or mail) to the appropriate STR and Heather.Caudill@pantex.doe.gov.
- Additional briefings for Pantex subcontractors and vendors may be requested from the Classification Office.

Accidental Release Issue Notification

- **Any release of UCNI/CUI, actual or suspected, MUST be reported to Pantex immediately, including inadvertent placement of information on uncertified systems or e-mail.**
  - Immediately notify the following:
    - Pantex Operations Center at 806-477-5000 (then you may call the buyer)
    - Be very generic in description (e.g., “This is Joe Smith. I am a vendor with Smith Associates, working the [Pantex] project and I’ve had an unauthorized release of protected information.”)
  - If Personally Identifiable Information (PII) release is suspected, notify the Pantex OC within **10 minutes.**
  - DO NOT e-mail or fax notification
  - DO NOT discuss details of UCNI release over telephone
- DO NOT attempt to “fix” the situation; contain situation only
- An Incident of Security Concerns (IOSC) representative will inquire, instruct, and remediate.

Finally…

- DO NOT relate your association with Pantex or the product which is delivered to any persons not directly involved with the task or contract without PRIOR WRITTEN APPROVAL from Pantex Procurement.
  - No postings to social networking sites or web locations without prior written approval
  - No references in brochures, proposals, or verbal confirmation without prior approval
- DO NOT discuss your involvement with Pantex in public.
- Be aware of persons with whom you discuss your involvement in the course of executing the task.
- Prohibited: Release of government-owned information is strictly prohibited without prior authorization. Failure to obtain authorization can result in fines or contract repercussions. If in doubt, contact the Information Release office (IRO).

- Last Step: Complete PX-6668, UCNI/CUI Protection Acknowledgment Form and submit it to your STR and the CUI official liaison for record. Heather.Caudill@Pantex.doe.gov

CNS | consolidated nuclear security, llc

UCNI / CUI Protection Acknowledgement Agreement

1. I will ensure:
   a. All UCNI / CUI is properly marked, handled, stored, transmitted, reproduced, and destroyed in accordance with CNS guidance and procedures.
   b. Access to UCNI / CUI is provided only to those individuals who are working on a CNS contract and possess the proper need to know/access authorization.
   c. No foreign nationals have access to UCNI / CUI unless otherwise authorized by CNS.
   d. Project information is discussed in authorized areas using appropriate devices. (Discussions in public locations are prohibited.)
2. I understand:
   a. Transmitting government owned CNS information outside of the CNS environment to non-certified systems is prohibited. All government owned CNS information must be processed on, and remain on the CNS certified system.
   b. My responsibility to immediately report potential or suspected incidents to the Y-12 Operations Center (formerly Plant Shift Superintendent Office) @ [illegible] or the Pantex Operations Center @ [illegible] immediately.
   c. Release of all government owned CNS information and CNS related information is strictly prohibited without prior authorization. Failure to obtain authorization can result in fines or termination of the contract.

I hereby acknowledge that I have reviewed CNS training "**Identification and Protection of UCNI / CUI at Facilities External to CNS**," and read and understand the CNS "**UCNI/CUI Protection Requirements for CNS Suppliers**" [illegible]. I understand it is my responsibility to comply with associated laws, federal regulations, and CNS policies and procedures to include DOE Order requirements for the protection and control of UCNI/CUI.

____
Printed Name

______________________ ______________
Signature Date

____
Company Name

- **Contact an expert if you have UCNI/CUI-related needs or questions:**
  - **UCNI Program Manager Marley Hoggatt, 806-573-6754, Marley.Hoggatt@Pantex.doe.gov**
  - **CUI Official Liaison Heather Caudill, 806-573-5658, Heather.Caudill@pantex.doe.gov**
  - **Privacy Officer John Garrett, 806-573-8400, John.d.Garrett@pantex.doe.gov**
  - **Export Control/Legal/Information Release Office: Shawn Hudson, 806-573-7567, Shawn.Hudson@Pantex.doe.gov**

As a reminder, this UCNI/CUI Information Protection training is required every two years!