



PANTEX PLANT | Y-12 NATIONAL SECURITY COMPLEX

Identification and Protection of UCNI / OUO / CUI at Facilities External to CNS

Revision 17 – 1 October 2023



Controlled Unclassified Information and UCNI

- The Department of Energy (DOE) has established the Controlled Unclassified Information (CUI) program
 1. DOE Order 471.7 'Controlled Unclassified Information ' (CUI) [Feb 2022] standardizes CUI across the DOE complex
 2. Former Official Use Only (OUO) Order and Manual (DOE O 471.3 and DOE M 471.3-1) are cancelled/superseded
 - i. OUO Information is now considered 'Legacy' information
- DOE O 471.1B 'Identification and Protection of Unclassified Controlled Nuclear Information' (UCNI) 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
- CNS CUI Program is managed by the CNS Office of the Chief Information Officer (OCIO) Information Solutions & Services (IS&S) with special advisory support through the CNS Classification Office



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 (2) 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



If Your Organization Has or is Using OUO Information

If Your Organization has OUO information or material from previous communications or projects

DOE CUI Waiver (dated 24 March 2022):

- Maintain existing marked OUO documents/materials in a controlled/record environment
 - If reuse of information is required, then material must be redesignated as CUI
- If OUO information transmission is required - it must be redesignated as CUI before transmission
- Refer to DOE O 471.7 for email transmission requirements
 - *Note 1: Same as OUO*
 - *Note 2: Continue to protect OUO & CUI*



Department of Energy
Washington, DC 20585

March 24, 2022

MEMORANDUM FOR ALL HEADS DEPARTMENTAL ELEMENTS

THROUGH: Ann Dunkin 
Chief Information Officer and Senior Agency Official for CUI
Office of the Chief Information Officer

FROM: Tonya Crawford Tonya D. Crawford
Acting Controlled Unclassified Information Program Manager Enterprise Records Management

SUBJECT: Waiver of Controlled Unclassified Information Marking Requirements for Legacy Information and Data

With the introduction of the new Department of Energy (DOE) Controlled Unclassified Information (CUI) program, unclassified information that requires safeguarding or dissemination control under law, regulation, or Government-wide policy is subject to the new CUI marking paradigm. This marking requirement extends to information that was marked as Official Use Only, or otherwise controlled, ("legacy information") before the CUI program went into effect. Pursuant to 32 CFR § 2002.38(b), in situations where an agency has a substantial amount of information with legacy markings and remarking it as CUI would be overly burdensome, the Senior Agency Official for CUI (SAOCUI) may approve a waiver of these requirements.

The digital and physical information assets of DOE are vast and applying the requirement to re-mark legacy information would be extremely burdensome in time and require significant financial resources. Therefore, under my authority as SAOCUI under 32 CFR § 2002.38, and as reflected in DOE Order 471.7, Controlled Unclassified Information, I hereby waive this marking requirement for legacy information from the date of this memo. Under this waiver, the Department is not required to remove legacy markings, and designate or re-mark it as CUI, as long as the information is not reused by the Department and remains under Departmental control. When the agency reuses any legacy information that qualifies as CUI, whether the information has obsolete control markings or not, the agency must designate the reproduced information as CUI and mark it accordingly.

This waiver will be reviewed on an annual basis for determination of continued applicability.



How to Redesignate OUO to CUI

Redesignate OUO Information to CUI

SUMMARY

Issue Date: March 8, 2016

Version 0

OFFICIAL USE ONLY

May be exempt from public release under the freedom of Information Act (5 U.S.C. 552), exemption number and category: 7, Law Enforcement
Name/Org: Joe Engineer, UPT Eng.
Date: 1/1/16
Guidance (if applicable): N/A



OFFICIAL USE ONLY

- If Marked OUO Ex 7 for Law Enforcement, or Ex 4 for Commercial/Proprietary - Redesignate to “**CUI**” centered at TOP and BOTTOM of Page
- Cover over previous OUO Signature box
- Cover OUO Marking at bottom with new marking
- Add a ‘Controlled By’ block with your name and date

Controlled By:
Your Name, ABC Contracting
Date: 25 Feb 2023

- Redesignated **CUI** looks like this:

CUI


Redesignate OUO Information to CUI

SUMMARY

Issue Date: March 8, 2016

Version 0

Controlled By:
Your Name, ABC Contracting
Date: 25 Feb 2023

 CUI

FOR TRAINING PURPOSES ONLY



Redesignate OUO/Export Controlled Information to CUI

- If Marked OUO Exemption 3 for Export Controlled Information, Redesignate markings to “**CUI//SP-EXPT**” centered at TOP and BOTTOM of Page
 - If “OUO”, “ECI”, “Export Controlled Information” or any combination of an ECI marking at bottom, cover it with new CUI marking
 - Cover over previous OUO Signature box
 - Add a ‘Controlled By’ block with your name and date

Controlled By:
Your Name, ABC Contracting
Date: 25 Feb 2023

- Redesignated **CUI//SP-EXPT** looks like this:

CUI//SP-EXPT


Redesignate Export Controlled Information to CUI

SUMMARY

Issue Date: March 8, 2016

Version 0

Controlled By:
Your Name, ABC Contracting
Date: 25 Feb 2023

 **CUI//SP-EXPT**



UCNI Markings Remain - No Change is Required

Marking Unclassified Controlled Nuclear Information (UCNI)

SUMMARY

Issue Date: March 8, 2016

Version 0

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

Reviewing Official: R. O. Reviewer/CNS UPF Security
(Name/Organization)

Date: 1/1/16

Guidance Used: CG-55-4

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

Reviewing Official: R. O. Reviewer/CNS UPF Security
(Name/Organization)

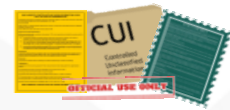
Date: 1/1/16

Guidance Used: CG-55-4

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

- If Marked UCNI, **There is NO CHANGE Required.** Maintain the UCNI marking centered at the **BOTTOM** of the page

UCNI / CUI Orders, Regulations and Policies



Applicable Law and DOE Regulatory Requirements

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

Applicable Procedures and Policies

E-PROC-0043	Exporting Compliance Procedure
E-PROC-3123	Identification and Protection of Unclassified Controlled Nuclear Information (UCNI) & Controlled Unclassified Information (CUI)
UCN 26608	UCNI / CUI Protection Requirements for CNS Suppliers

Access to UONI and CUI



- **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 Y-12, UPF or Pantex when requested.
 - Acceptable documents include:
 - 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
- **Must be briefed on protection requirements prior to being provided access (i.e. Completion of this briefing followed by signed acknowledgement agreement)**
- **UCNI Access 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
- **CUI Access eligibility is based on Law, Regulation, Government-wide Policy**

Access to UCNI and CUI (cont.)



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 utilized for the processing of UCNI / CUI must have the means to protect the information from unauthorized viewing and 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 UCN 26608 for more details

The less people you have handling UCNI/CUI the better

Access to UCNI and CUI (cont.)

UPF Only



Uranium Processing Facility (UPF) Oak Ridge Tennessee, Subcontract Pre-Award Activity

• Bidder Preparation and Submission of Proposals

- As a prospective bidder to a UPF Request for Proposal (RFP), you may receive hard-copy UCNI / CUI documents from the Buyer (UPF) after completion of this training module
- You will also receive UCN-23304, *UPF CUI Subject Matter Determination* form that lists specific UCNI/CUI subject areas that you **MUST** avoid during preparation of your proposal
- **DO NOT include references to these UCNI / CUI subject areas in your proposal**
- **DO NOT process information related to these UCNI subject areas on computers that have not been certified for UCNI processing**
- See example of the blank UCN-23304, *UPF CUI Subject Matter Determination* on the next slide

Access to UCNi and CUI (cont.)

UPF Only



UPF CUI SUBJECT MATTER DETERMINATION

RFP MR:		Date:
Applicable CUI Category: <input type="checkbox"/> OUO <input type="checkbox"/> UCNi		
CUI SUBJECT AREAS		
<u>ATTENTION BIDDERS:</u> <i>Do Not Include References To Information Below In Bid Package Or Process Any of the Topical Areas Below on Uncertified Computers.</i>		
APPROVAL		
UPF Security Procurement Support:	_____	_____
	Printed Name/Signature	Date
UPF Procurement:	_____	_____
	Printed Name/Signature	Date
CONCURRENCE		
CNS Classification:	_____	_____
	Printed Name/Signature	Date
UPF Security Support Manager:	_____	_____
	Printed Name/Signature	Date

UCN-23304 (03-27-18)
Y19-95-207



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

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



Processing UCNI on Computers

Computer and/or other equipment processing UCNI

- Computer requires certification by Pantex/Y-12 Cyber Security 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 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 Cyber Security before processing UCNI.** Those who have access to the stand-alone / network must meet access and training requirements
- All storage media (e.g., hard drive, CDs, DVD's, etc.) must be encrypted, removable, and able to be surrendered upon termination of the contract. Media (including back-up media) must be provided to Cyber Security at completion of task or contract. Media must be marked according to instruction

NOTE: Request for computer certification is after award of contract

Processing UCNI on Computers (cont.)



Computer or other equipment processing UCNI

- Operating System must meet requirements of Cyber Security. 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 Cyber Security 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 Cyber Security
- **Prohibited:** Attachment to or use of corporate, company, or public networks or personal email to process UCNI is **prohibited** unless approved and documented by Cyber Security. **UCNI 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 Cyber Security 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 Cyber Security
- 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 government-furnished-equipment (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 CNS Cyber Security 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/Y-12 property is prohibited without express written approval from Cyber Security.

Marking UCNI Documents



- **Marking of UCNI Documents pending classification review**
 - Documents generated from a certified UCNI-approved computer requires 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 documents 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 have at least one DOE trained DC/RO within the organization. Details on how to become a DC/RO can be obtained through the Y-12 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 prior to and preceding the fax

• Electronic mail

- **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 Y-12 Classification Office UCNI Program Manager 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

- **DO NOT** 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
- **DO NOT** 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 in Pantex approved Shred Box or a Y-12 approved DAR Bin (coordinate with STR) “protect as UCNI” procedures (i.e. locked room, or cabinet) until given to STR for proper destruction” (Preferred)
- Shred all UCNI/CUI paper documents in a crosscut shredder
 - UCNI law currently allows no greater than ¼ inch wide x 2 inches long
 - However, UCNI should be shred to meet CUI requirements: 1mm x 5mm

Important points concerning shredders:

- A shredder is a piece of equipment that needs to be properly maintained and cared for. Refer to your shredder owner’s manual for how to routinely clean your shredder and oil its cutting blades
- Monitor the collection bin, and empty as necessary; ensure paper flows freely through cutting blades
- Know your shredder’s maximum sheet capacity. Trying to shred more pieces of paper at one time than your shredder’s maximum capacity will result in shred residue that is out of compliance
- Check shred residue after every use to ensure compliance. If out of compliance immediately take it of service and protect all UCNI/OUO information accordingly until a new shredder is procured
- **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 destroyed per instructions and other matter has been returned to Pantex/Y-12 for further disposition

NOTE: If media or non-paper items cannot be shredded due to the material (e.g., plastic, transparencies, metal), they must be returned to your STR for further disposition

Briefing Requirements



- Each member of your team (including lower tier subs and vendors) must receive this briefing if they will be handling UCNI/CUI.
- Maintain a record of briefing including date of briefing, instructor, printed name and signature of individual being briefed
 - Maintain a copy of briefing record (acknowledgement form)
 - Provide a copy of the acknowledgement form (via pdf, fax, or mail) to the appropriate STR and Steven.Aragon@pxy12.doe.gov
- Briefings for Pantex and Y-12 subcontractors and vendors may be requested
- Briefings for UPF subcontractors and vendors may be requested
- Contact an expert if you have UCNI / CUI related needs or questions
 - Y-12 / Pantex
 - UCNI Program Manager: Steven Aragon, 865.241.4995, Steven.Aragon@pxy12.doe.gov
 - CUI Official & Privacy Officer: Jai Sharma, 865.574.8703, Jai.Sharma@pxy12.doe.gov
 - Export Control/Legal: Sara Webb, 865.574.5360, Sara.Webb@pxy12.doe.gov
 - UPF
 - UPF Security: Chris West, 865-241-4783, Christopher.West@pxy12.doe.gov



Accidental Release Issue Notification

- Any release of UCNI / CUI, actual or suspected, **MUST** be reported to Pantex/Y-12 immediately, including inadvertent placement of information on uncertified systems or e-mail
 - Immediately notify:
 - Y-12 Operations Center (OC) [formerly known as the Plant Shift Superintendent (PSS)] at 865-574-7172, or
 - 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 [Y-12, Pantex or UPF] project and I’ve had an unauthorized release of protected information.”***
 - If Personally Identifiable Information (PII) is suspected, notify the Y-12 or Pantex OCs 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 [Y-12, Pantex, UPF] or the product which is delivered, to any persons not directly involved with the task or contract, without **PRIOR WRITTEN APPROVAL** from CNS 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 Y-12, UPF or 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) at 865-574-5360 or IRO@pxy12.doe.gov
- **Last Step: Complete the “UCNI / CUI Protection Acknowledgement Form” and Submit it to the UCNI Program Manager for record**

CNS consolidated nuclear security, inc.
 10000 E. Highway 100, Suite 1000, Livermore, CA 94550
 (925) 434-2000

UCNI / CUI Protection Acknowledgement Agreement

I, the undersigned, hereby acknowledge that I have received CUI training, "Identification and Protection of UCNI / CUI" and understand the "UCNI / CUI Protection Requirements for the Supplier". I understand it is my responsibility to comply with associated laws, federal regulations, and CNS policies and procedures to include CUI/UCI/UCR requirements for the protection and control of UCNI/UCI.

I understand that I have received CUI training, "Identification and Protection of UCNI / CUI" and understand the "UCNI / CUI Protection Requirements for the Supplier". I understand it is my responsibility to comply with associated laws, federal regulations, and CNS policies and procedures to include CUI/UCI/UCR requirements for the protection and control of UCNI/UCI.

Printed Name: _____
 Signature: _____ Date: _____
 Company Name: _____