

CNS | consolidated nuclear security, llc
PANTEX PLANT | Y-12 NATIONAL SECURITY COMPLEX

Identification and Protection of UCNI / OUO Information at Facilities External to CNS (Pantex, Y-12 & UPF)

Revision 15 – March 09, 2021

This document has been reviewed by a CNS Dual Authority DC/RO and confirmed to be UNCLASSIFIED and contains no UCNI.
Name: Steven Aragon
Date: 03/09/2021
CNS eDC/RO ID: 290774

Controlled Unclassified Information

- **Currently within the Department of Energy (DOE) and The National Nuclear Security Administration (NNSA), the term Controlled Unclassified Information (CUI) has dual meanings**

  1. **An overarching term used to refer to unclassified information that is identified and marked as sensitive (e.g. UCNI, OUO, and PII)**
  2. **Used to describe information that will eventually be identified and safeguarded under 32 CFR 2002, which mandates a U.S. Government-wide uniform program to identify and protect sensitive, but unclassified information**

- **At this time DOE/NNSA has not established policies for identifying and protecting CUI in accordance with the new published CFR, and a timetable for implementation within DOE/NNSA has not been established**

- **DOE Office of Classification has directed all contractor and federal employees to continue to identify and protect UCNI, OUO and PII in accordance with already established DOE Orders and federal regulations**

- **Protection of this information within CNS will be addressed as The CNS UCNI/OUO Information Protection Program with PII being considered Official Use Only (OUO) information**

Categories of Protected Information

- **Official Use Only (OUO):** Unclassified information determined to be sensitive under the Freedom of Information Act (FOIA) and protected as sensitive but not otherwise controlled. This category includes Export Controlled Information (ECI) as well as Personally Identifiable Information (PII) which is a name associated with date of birth, social security number, or other personal information not publically available
- **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, and the adverse effect of release of such materials or 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 (ECI):** 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. ECI technology and products are controlled to prevent unauthorized release to foreign countries, organizations, or individuals

Examples of Markings - OUO

Use of Official Use Only (OUO) Information

SUMMARY

Issue Date: March 8, 2016

Version 0

EXAMPLE

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, UPF Eng.
Date: 1/1/16
Guidance (if applicable): N/A

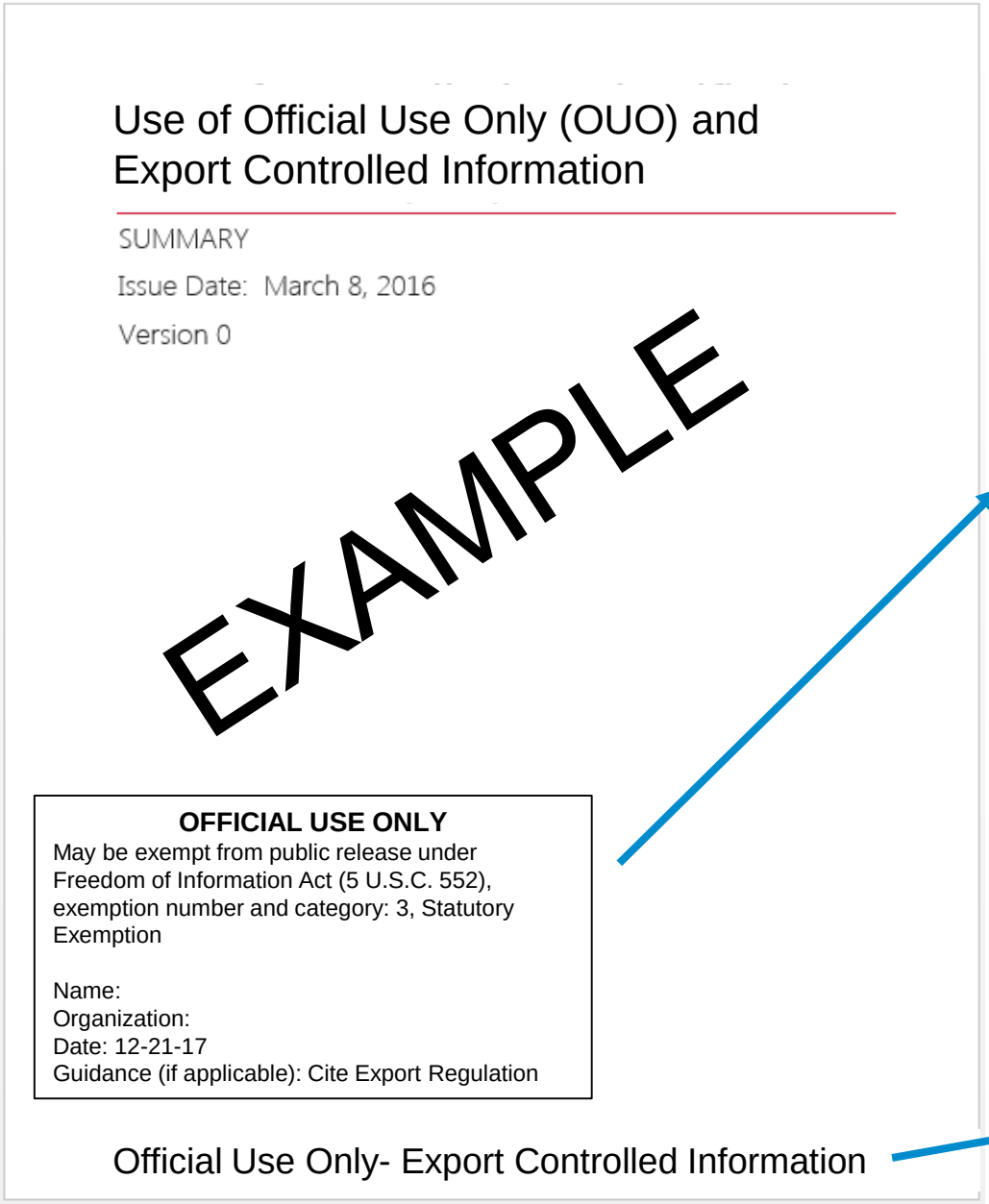
OFFICIAL USE ONLY

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, UPF Eng.
Date: 1/1/16
Guidance (if applicable): N/A

OFFICIAL USE ONLY

Examples of Markings – OUO-Export Controlled Information

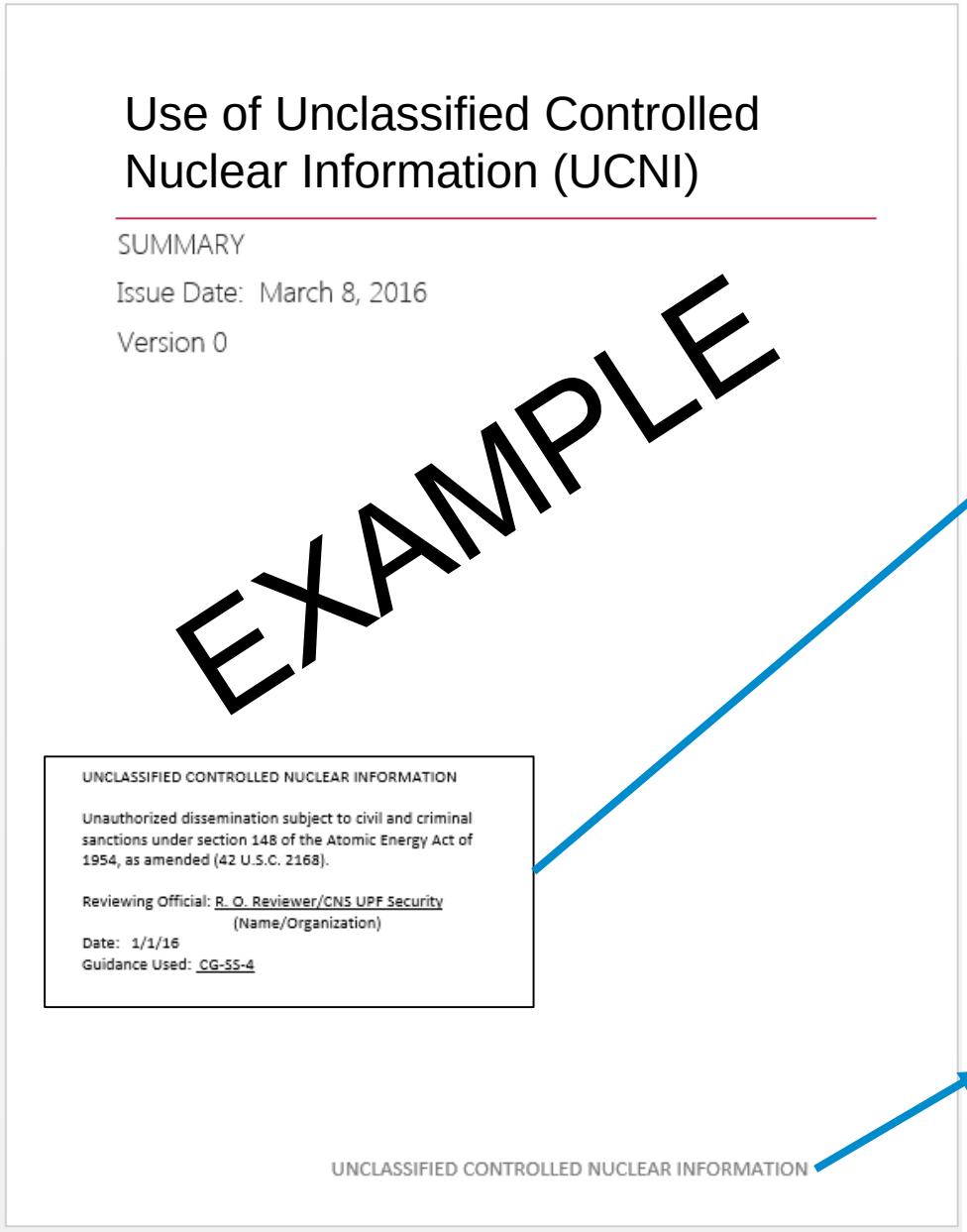


OFFICIAL USE ONLY
May be exempt from public release under Freedom of Information Act (5 U.S.C. 552), exemption number and category: 3, Statutory Exemption

Name:
Organization:
Date: 12-21-17
Guidance (if applicable): Cite Export Regulation

"OFFICIAL USE ONLY-ECI" on the bottom of each page that contains ECI

Examples of Markings - UCNI



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-SS-4

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

UCNI / OUO Orders, Regulations and Policies

Applicable 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 471.3	Identifying and Protecting Official Use Only Information
DOE M 471.3-1	Manual for Identifying and Protecting Official Use Only

Applicable Procedures and Policies

Y19-401	Automated Information System (AIS) Security Handbook (OUO)
Y15-404	Acceptable Use of Information Technology Equipment
MUN08-00051-01, Rev. 1.0.03	Unclassified Master Information System Security Plan (Unclassified-ISSP)(OUO)
CNS E-PROC-0043	Exporting Compliance Procedure
UCN 26608	UCNI / OUO Information Protection Requirements for CNS Suppliers

Access to UCNI / OUO Information

- **<u>Does not</u> require a clearance**
- **Must be a citizen of the United States (Cannot be a Foreign National)**
  - 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 raised and/or colored 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
  - *Non-US Citizens may qualify for access through meeting certain criteria*
- **Must be briefed on protection requirements prior to being provided access. (i.e. Completion of this briefing followed by signed acknowledgement agreement)**
- **Access limited to need-to-know**
  - 'Need-to-know' means an individual who 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 / OUO Information (cont.)

Access must be controlled

- While in use, the Authorized Individual or person granted limited access must maintain physical control over any UCNI / OUO information 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 individual
- Handling or processing:
  - MUST be performed in a facility's closed, unobservable office or area
  - MUST NOT be in public areas or areas susceptible to casual viewing
- **UCNI / OUO Information work areas and computers that are utilized for the processing of UCNI / OUO information must have the means to protect the information from unauthorized viewing and configured to resist unauthorized entry**
- While in transit, documents must be packaged to conceal information and must remain under individual's positive control.

The less people you have handling UCNI/OUO Information the better

NOTE: No Y-12, UPF or Pantex information, including Unclassified Non-sensitive, may be shared with foreign nationals without prior approval

Access to UCNI / OUO Information (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 / OUO 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/OUO subject areas that you MUST avoid during preparation of your proposal
  - **DO NOT include references to these UCNI / OUO subject areas in your proposal**
  - **DO NOT process information related to these UCNI / OUO subject areas on computers that have not been certified for UCNI / OUO processing**
  - You will find an example of the blank UCN-23304, *UPF CUI Subject Matter Determination* on the following page.

Access to UCNI / OUO Information (cont.)

UPF Only

UPF CUI SUBJECT MATTER DETERMINATION

RFP MR:		**Date:**
Applicable CUI Category:	☐ OUO ☐ UCNI	
CUI SUBJECT AREAS		
ATTENTION BIDDERS: *Do Not Include References To Information Below In Bid Package Or Process Any of the Topical Areas Below on Uncertified Computers.*		
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 / OUO documents to lower-tiers after the BUYER's approval

- **Lower-tier subcontractors are held to the same requirements prior to receiving UCNI / OUO information**
  - **Citizenship**
  - **Protection measures**
  - **Training**
  - **Need to know**

- **SUBCONTRACTOR** is responsible to ensure lower-tiers meet re-training and re-certification requirements

As a reminder, UCNI / OUO Information Protection training is required <u>every two years</u>

Processing UCNI / OUO Information

Computer and/or other equipment processing UCNI / OUO Information

- Computer requires certification by CNS Cyber Security prior to use:
  - Certification duration is 3 years with annual verification of status at 1 and 2 year dates during certification period
  - Certification includes all protected information up to and including UCNI
- Computer must be stand-alone with no network (air-gapped) or attached to stand alone network (air-gapped network), **and must be certified by CNS Cyber Security before processing UCNI/OUO**. All those who have access to the stand-alone or the network must meet access requirements, including training for ISSOs
- 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 CNS 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 / OUO Information (cont.)

Computer or other equipment processing UCNI / OUO Information

- Operating System must meet requirements of CNS 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 CNS 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 CNS Cyber Security
- Prohibited: Attachment to or use of corporate, company, or public networks or personal email to process UCNI / OUO information is **prohibited** unless approved and documented by CNS Cyber Security. UCNI / OUO Information placed on an unapproved system is an Incident Of Security Concern (IOSC) and may result in fines or contract termination
- Prohibited: Wireless capabilities are **prohibited** unless CNS Cyber Security directed FIPS standards are used and permission through the CNS Telecommunications Proposal process is granted

Processing UCNI / OUO Information (cont.)

Computer or other equipment processing UCNI / OUO Information (cont.)

- Passwords must conform to DOE requirements and be provided by CNS Cyber Security
- Use of PDAs, PC Tablets, Blackberries, etc., for processing CNS information require special handling and approval through the CNS Telecommunications Proposal process. Permission may not be granted
- **Only authorized personnel may have access to computer(s) when processing UCNI / OUO information. Computer(s) may be accessed by others when not being used to process UCNI / OUO information and requisite media 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 / OUO information
- If a subcontractor is supplied CNS government furnished equipment (GFE) (often referred to as a GFE laptop) at no time can any information, UCNI / OUO or Unclassified, be moved from the GFE laptop to a non-federal corporate network. CNS information (UCNI / OUO or Unclassified) may only be moved from a GFE laptop to an air-gapped system that has been certified and accredited by the UCNI / OUO Information Protection Cybersecurity Team Lead or UPF Cybersecurity POC, and back to the GFE laptop if necessary using an encrypted “IronKey” USB storage thumbdrive

NOTE: Use of Wi-Fi hotspots on CNS property is prohibited without express written approval from CNS Cyber Security.

Marking UCNI Documents

- **Marking of UCNI Documents pending classification review**
  - Documents generated from a certified UCNI / OUO-approved computer requires protection at the highest level of certification (i.e., UCNI) pending classification review
  - Only a CNS Derivative Classifier/UCNI Reviewing Official (DC/RO) can make a determination of the documents sensitivity. Contact your 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 / OUO information, it's **highly recommended** that your organization have at least one DOE trained DC/RO within the organization. Details on how to become a DOE DC/RO can be obtained through the CNS Classification Office
  - Hard copy documents from UCNI / OUO-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 / OUO-approved computers **MUST** be protected as UCNI if the document is in draft until a CNS DC/RO has made a determination. Final documents in electronic format must be marked UCNI if so determined by a DC/RO

Transmitting UCNI / OUO Information

- **Telephone**
  - **DO NOT** Discuss:
    - UCNI over telephone. Secure phone (OMNI or STE) must be used
    - OUO or ECI over VOIP, cordless, or cellular telephones. May only use a landline for these discussions
- **Facsimile**
  - **DO NOT** fax UCNI
  - Faxing is permitted for OUO and ECI 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/OUO without CNS approved encryption and certification
    - UCNI/OUO to computers that have not been certified for use
  - **DO NOT** use file services (e.g., Dropbox), social networking sites (e.g., Twitter, Facebook, etc.), or other non-CNS approved methods for transmitting government-owned CNS information. **This includes all Y-12, UPF or Pantex information to include Unclassified Non-sensitive information**

Transmitting UCNI / OUO Information (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.)

Reproducing UCNI / OUO Information

- **Reproduction**
  - Reproduction of UCNI / OUO information 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 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 / OUO Information

Destruction

- Place in Pantex approved Shred Box (get from STR) “protect as UCNI” procedures (i.e. locked room, or cabinet) until given to STR for proper destruction” (Preferred)
- Shred all UCNI/OUO paper documents in a crosscut shredder with residue no greater than ¼ inch wide x 2 inches long

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
- If your shredder has an additional slot used exclusively for the destruction of compact disks (CDs), cover this slot and mark on it “DO NOT USE”
- 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 CNS 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/OUO information. 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 CNS acknowledgement form (via pdf, fax, or mail) to the appropriate CNS STR and Dale.Dugger@cns.doe.gov
- **Briefings for CNS Pantex and Y-12 subcontractors and vendors may be requested**
- **Briefings for UPF subcontractors and vendors may be requested**

- **Contact your security representative if you have UCNI / OUO related needs or questions**
  - **Y-12 / Pantex**
    - **Steven Aragon, 865.241.4995, Steven.Aragon@cns.doe.gov**
    - **Dale Dugger, 865.241.2058, Dale.Dugger@cns.doe.gov**
  - **UPF**
    - **Chris West, 865-241-4783, Christopher.West@cns.doe.gov**

Release Issue Notification

- **Any release of UCNI / OUO information, actual or suspected, MUST be reported to CNS 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**
- **A CNS Incident of Security Concerns (IOSC) representative will inquire, instruct, and remediate**

Finally…

- **<u>DO NOT</u> relate your association with [Y-12, Pantex, UPF, CNS] or the product which is delivered, to any persons not directly involved with the task or contract, without PRIOR WRITTEN APPROVAL from the CNS Procurement Authority**
  - No postings to Social Networking sites or other web locations without prior written CNS
  - No references in brochures, proposals, or verbal confirmation without prior written CNS approval
- **<u>DO NOT</u> discuss your involvement with Y-12, UPF or Pantex in public**
- **<u>Be aware</u> of persons with whom you discuss your involvement in the course of executing the task**
- Prohibited: **Release of all government owned CNS information is strictly prohibited without prior authorization. Failure to obtain authorization can result in fines or termination of contract. If in doubt contact the CNS Information Release office (IRO) at 865-574-5360 or IRO@CNS.DOE.GOV**
- **All requirements in this briefing apply to lower-tier subcontracts/vendors**
- **Next Step: Complete the UCNI / OUO Training Acknowledgement Form and Submit it to the UCNI / OUO Team for record**