UCNI / OUO Information Protection Requirements for CNS Suppliers

Subcontract contains **UCNI** ☐ **OUO** ☐ **Both** ☐

Protection of UNCI / OUO Information

SELLER shall be responsible for protecting all Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO) Information, and materials in connection with the performance of the work under this Purchase Order and in accordance with the CNS UCNI/OUO Information Protection Program requirements outlined in Appendix A. SELLER shall protect against sabotage, espionage, loss, and theft of UCNI/OUO information and/or materials in SELLER's possession. UCNI/OUO information will be protected in accordance with the U.S. Department of Energy/National Nuclear Security Administration (DOE/NNSA) Classification Program, CNS Cyber Security Program Plan (CSPP) and the CNS UCNI/OUO Information Protection Program outlined in Appendix A.

Definitions

Access authorization	An administrative determination that an individual is eligible for access to sensitive matter.
Automated Information System (AIS)	An assembly of computer equipment, facilities, personnel, software, and procedures configured for sorting, calculating, computing, summarizing, storing, and retrieving data and information.
AIS Equipment	All computer equipment, peripherals, software, data, networks, and facilities.
AIS security incident	A failure to comply with AIS security requirements, which results in attempted, suspected, or actual compromise of Controlled Unclassified Information.
AIS Security Plan	A document that describes the protection of sensitive AIS against unauthorized disclosure, modification, or destruction of the system or data, and denial of service to process data, including physical, personnel, administrative, telecommunications, hardware, and software security features.
AIS storage media	A means used by AIS systems to convey or store information.
Computer Security Officer (CSO)	SELLER person(s) responsible for the implementation of their AIS Security Plan.
Controlled Unclassified Information (CUI)	Currently within the Department of Energy (DOE) and The National Nuclear Security Administration (NNSA), the term Controlled Unclassified Information (CUI) has dual meanings. One, it's an overarching term used to refer to unclassified information that is identified and marked as sensitive (e.g. UCNI, OUO, and PII). Secondly, the term is also 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. However, 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. Therefore, the 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.

Export Controlled Information (ECI)	ECI is scientific and technical information or commodities that are controlled by the Department of Commerce, Department of Energy, Department of State, Nuclear Regulatory Commission, and the Atomic Energy Act of 1954. The goal of the federal export laws laid out by these agencies is to control the unauthorized release of technology and commodities to foreign entities (Foreign companies, foreign person, foreign governments)
FIPS – Federal Information Processing Standards.	Standards and guidelines issued by the National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS) for use government-wide. Specifically, applicable FIPS standards are included in FIPS 140-2.
Incident of Security Concern	A knowing, willful, or negligent action contrary to the requirements for information security.
Information Security (INFOSEC)	A system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information for which protection has been authorized.
Information Security Point of Contact (POC)	SELLER person(s) responsible for the implementation of requirements to avoid unauthorized disclosure of information.
Label	The marking of an item of information to reflect the sensitive information (e.g., UCNI, OUO, etc.).
Need-to-Know	A risk based decision by an authorized person having responsibility for sensitive information that a prospective recipient requires access to information in order to perform official, approved, authorized tasks or services.
Official Use Only (OUO)	Unclassified sensitive information which may be exempt from public release under the Freedom of Information Act (FOIA).
Security Plan	A document that describes the protection of the facility and/or its assets.
Unclassified	The designation for information, a document, or material that has been determined not to be classified or that has been declassified by proper authority. The information is not publicly releasable unless authorized by the BUYER. The information, document, or material may require additional protection if designated as Controlled Unclassified Information.
Unclassified Controlled Nuclear Information (UCNI)	Certain unclassified government information prohibited from unauthorized dissemination as defined by the Atomic Energy Act of 1954, Amended.

SELLER Responsibilities

- Ensure all personnel handling UCNI/OUO information have completed the required **on-line briefing** and **acknowledgement agreement** for protection of UCNI/OUO information provided by the UCNI/OUO Information Protection team at the following website: https://pantex.energy.gov/about/visiting-us/visitor-training
- Ensure UNCI/OUO information is granted only to U.S. Citizens with a valid need-to-know and is not released without review for release restrictions;
- Ensure UCNI/OUO information is never released to foreign nationals;

- Ensure UCNI/OUO information is not placed on the SELLER's computing equipment without prior approval of the SELLER's Information System Security Plan (ISSP) by CNS Cybersecurity;

- Immediately notify the Y-12 Operations Center (OC) [formerly known as the Plant Shift Superintendent] at 865-574-7172, or the Pantex Operations Center at 806-477-5000 of any known or suspected security breaches

- Be responsible for recognizing the sensitivity of information before it is stored, processed, or transmitted on any information system; UCNI/OUO information can only be stored, processed or transmitted on a system approved by CNS Cybersecurity.

- Return to the BUYER all UCNI/OUO storage media (disk drives, thumb drives, hard drives) in SELLER'S possession or in the possession of any person under the SELLER'S control in connection with the performance of a subcontract are returned to the BUYER in conformance with CNS specifications upon completion of the Purchase Order.

- Ensure all hard copy UCNI/OUO information is returned to the Buyer or STR when no longer contractually required or properly destroyed with a statement of destruction provided.

- Flow these requirements down to all lower-tier subcontractors and/or suppliers. Ensure lower-tier subcontractors and/or suppliers are approved by the BUYER prior to providing electronic or hard copy UCNI or OUO information.

Requirements

CUI Handling and Protection Briefing Requirements

SELLER is personally responsible for safeguarding, handling, possessing, or processing UCNI or OUO information and must first successfully complete the UCNI/OUO Information Protection briefing provided by the CNS UCNI/OUO Information Protection Program. SELLER's lower-tier subcontractors and/or suppliers are also required to complete the same requisite briefing prior to being provided access to UCNI/OUO Information. The SELLER shall be responsible for coordinating any additional personnel for the briefing. The SELLER will provide the BUYER with briefing records of all individuals briefed including lower-tier subcontractors and/or suppliers upon request. The SELLER shall be responsible for the control of the UCNI/OUO documents and media and is not relieved of this obligation for documents provided to others. The UCNI/OUO briefing is required to be administered biennially (i.e., within 24 months of the initial briefing). SELLER must maintain current UCNI/OUO Information Protection briefing records for all SELLER personnel responsible for safeguarding, handling, possessing, or processing UCNI/OUO Information. Additional briefings or instructions may be directed by the BUYER at the BUYER's discretion.

Access to UCNI / OUO Information

Access to UCNI/OUO Information shall be provided only to those authorized for routine access in accordance with 10 CFR 1017 (U.S Citizens with valid need to know). Routine access refers to the normal exchange of UCNI/OUO information during the conduct of official DOE/NNSA business. An authorized individual, who may be the originator or possessor of UCNI/OUO, may grant routine access to UCNI/OUO information to another person eligible for routine access to the information by giving that person UCNI/OUO documents and providing assurance that the requirements below are met:

- Individual has completed the required on-line briefing provided by a CNS UCNI/OUO Information Protection Team

- Must be a citizen of the United States. Non-U.S. citizens (i.e., foreign nationals) are not allowed any access, casual or otherwise, to UCNI/OUO information or media. Verification of U.S. Citizenship must be determined, and a copy of the document retained by the SELLER, by one of the following:

1. Birth Certificate (certified copy with raised and/or colored official seal - issued by government/municipality [not issued by hospital])
2. Certificate of naturalization (Immigration and naturalization Services (INS) Form N-550 or N-570),
3. Certificate of U.S. Citizenship (INS Form N-560 or N-561),
4. Report of Birth Abroad of a citizen of the United States of America (Form FS-240), or
5. U.S. Passport (active with picture that still looks like the person).

- Access limited to need-to-know. A person must possess a valid "need to know" for the specific UCNI/OUO information in the performance of official duties. (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.

UCNI/OUO Information Work Area and/or Computer Equipment Approval

UCNI/OUO information must be controlled at all times to preclude unauthorized access. If SELLER must establish an **UCNI/OUO processing area** at the SELLER's location, notification must be submitted by the SELLER to the BUYER who will contact the CNS UCNI/OUO Information Protection Team so that liaison with the SELLER may be established in certifying the SELLERS UCNI/OUO processing area.

If SELLER desires to use **Automated Information Systems** (AIS) to process UCNI/OUO information electronically, an AIS Certification Request must be submitted to the BUYER and forwarded to the UCNI/OUO Information Protection Team. Certification is documented via an Information Systems Security Plan that details the information system controls used to protect information systems in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. It is the responsibility of the SELLER to know and provide the degree of protection required for the type of information being processed as advised by the UCNI/OUO Information Protection Team, CNS Cybersecurity and NIST SP 800-171. An Information System Security Plan shall be prepared and approved for each system that processes UCNI/OUO information.

Once the SELLER requests an UCNI/OUO information processing area approval and/or AIS approval, the BUYER will contact the SELLER to ensure appropriate protection measures are in place and will schedule an inspection 30 days prior to need. **Therefore, it is imperative that the SELLER submit the approval request and associated security plan as early as possible to allow sufficient time to schedule an approval inspection prior to need.**

Approval by UCNI/OUO Information Protection Cybersecurity Team Lead and CNS Cybersecurity is required prior to use or electronic processing of UCNI/OUO information at the SELLER's location. Modifications to the SELLER's protection measures and/or Information System Security Plan must be approved by CNS Cybersecurity prior to implementation. The UCNI/OUO Information Protection Team, CNS Cybersecurity and/or National Nuclear Security Administration Production Office (NPO) will perform regular and unannounced surveillances relative to approved information, computer, and physical protection plans.

The CNS UCNI/OUO Information Protection Team and CNS Cybersecurity approval is required prior to commencing construction, modification, or declaration of an UCNI/OUO information processing area or computer equipment.

Physical Security Requirements

UCNI/OUO information documents shall be kept in a secure place at all times to preclude unauthorized viewing and disclosure. Only locations that meet the following physical security requirements will be approved by the BUYER to store and/or process UCNI/OUO information. SELLER must ensure the following physical security measures are met:

- Must have internal building security (i.e., access control to the facility, area, or room in which UCNI/OUO information is stored or processed, such as by-name badge reader control, controlled key locks, etc.)
- Access control system must be controlled by the information security point of contact to ensure only individuals with appropriate U.S Citizens with valid need to know are allowed access.
- Windows must not allow viewing from outside into the room when processing UCNI/OUO information. This can be accomplished by using opaque coverings, closed blinds, etc. Windows must remain locked from the inside.
- Telephones (landline, VOIP, or cell) are allowed within the room, HOWEVER,
    - ECI and OUO – May only use a LANDLINE phone
    - UCNI – Requires a Secure phone (OMNI or vIPer)
- Areas may be used for other tasks associated with subcontractor when all UCNI/OUO matter is locked in separate lockable containers. If the perimeter of the area is access controlled due to the entire area being a UCNI/OUO area, it may not be used by others.
- Network drops
    - More information will be provided by the CNS Cybersecurity during the approval of the Seller's information systems and CUI processing area.
- Personal Workstations

  For personal computer workstations, the primary security feature is physical access control for the information. Access to the computer may be further restricted by the hardware and software controls as follows:
    - In offices with lockable doors and resistant to surreptitious entry, no hardware security devices are required as long as the room is locked when unattended. Alternative options will be considered by the CNS Cybersecurity and must be documented in the AIS Security Plan.
    - In open offices and where there is not a common need-to-know of all information, appropriate protective measures (e.g., chassis locks, keyboard locks, monitor shields, or approved hardware password devices) are required as directed by CNS Cybersecurity.
- Locations of monitors, printers, and other output devices
    - The monitor, printer, and any other output device of an AIS processing UCNI/OUO information shall be positioned to prevent casual viewing by unauthorized personnel.

Automated Information System (AIS) Requirements

UCNI/OUO information provided by the BUYER and deliverables or working materials provided by the SELLER in support of the Purchase Order shall be performed on BUYER certified AIS resources unless otherwise directed in writing by the UCNI/OUO Information Protection Team and shall operate in compliance with an CNS Cybersecurity approved AIS Security Plan. SELLER must meet the specific cyber security requirements, below, and in Appendix A, as applicable. SELLER shall submit a request for a certification inspection to the BUYER in accordance with previous guidance.

- <u>Computer Media and Encryption Requirements</u>
    1. Computer media containing UCNI/OUO information at the SELLER's facility and at lower-tier subcontractors' facilities shall be dedicated to this work. Lower-tiered subcontractor facilities and AIS must be approved by the BUYER prior to SELLER releasing UCNI/OUO information. UCNI/OUO information requires removable media including boot drives and drives which data is contained. In cases where UCNI/OUO information is contained on removable media (e.g.,

removable hard drives), a machine may be used for other purposes; however, all media must be removable, including boot drives.

2. System hardware components shall be marked to indicate the most restrictive category of information processed, as directed by the BUYER (UCNI/OUO Information Protection Team).
3. All media must be encrypted by BUYER approved FIPS 140.2 Level 1 or higher encryption methods.
4. If required, the SELLER shall install encryption software in compliance with BUYER (UCNI/OUO Information Protection) instructions.

An AIS processing UCNI/OUO information shall be re-approved by the BUYER (UCNI/OUO Information Protection) every three (3) years or when changes occur that affect the security posture of the system. A configuration modification of hardware, system software, or layered products may be cause for recertification of a system. The BUYER (CNS Cybersecurity) must approve modifications that change the security posture of a system prior to implementation. This includes new computing systems or networks to be connected to existing approved networks. They shall be documented and approved by the BUYER (CNS Cybersecurity) before connection and use.

1. Owners of data are responsible for recognizing the sensitivity of information before it is used, processed, or stored on an information system and for ensuring the system is certified for the information.
2. Protect UCNI/OUO information to which they have access or custody in accordance with security requirements identified in this document.

SELLER UCNI/OUO Information Protection Security Point(s) of Contact

- UCNI/OUO Information Protection Security Point of Contact (POC)

  The SELLER shall identify to the BUYER a qualified individual who is a citizen of the United States, and an alternate, to serve as the principal Point of Contact (POC) between the BUYER and the SELLER regarding UCNI/OUO information protection. The responsibilities of the position include but are not necessarily limited to:

  1. Representing the SELLER/lower-tier subcontractors and/or suppliers concerning UCNI/OUO Information Protection issues.
  2. Ensuring implementation of, and compliance with, all UCNI/OUO information protection requirements.
  3. Reporting security-related incidents to the BUYER (Y-12 Operations Center - 865-574-7172 or Pantex Operations Center – 806-477-5000 during off hours) and participating in the inquiry of security incidents.
  4. Determining UCNI/OUO Information Protection briefing/training needs and ensuring briefing/training is conducted in a timely manner.
  5. Disseminating periodic UCNI/OUO information protection awareness material to employees who have responsibilities that include protection and control of UCNI/OUO information.
  6. Attending meetings and briefing/training sessions as requested by the BUYER.

- Computer Security Point of Contact (POC)

  The SELLER shall identify to the BUYER a qualified individual and alternate to serve as the principal point of contact between the BUYER and the SELLER regarding computer security. The SELLER Computer Security POC is responsible for:

  1. Ensuring the implementation of, and compliance, with the AIS Security Plan.
  2. Representing the SELLER/lower-tier subcontractor and/or supplier for computer security issues.

3. Coordinating general AIS security briefings/trainings.
4. Reporting AIS-related security incidents to the BUYER (at Y-12 Plant Shift Superintendent's Office - 865-574-7172 or Pantex Operations Center – 806-477-5000 during off hours) and participating in the inquiry of cyber security incidents.
5. Coordinating the approval of computer systems processing UNCI/OUO information with the BUYER (CNS Cybersecurity).
6. Ensuring that the AIS system described by the AIS Security Plan has been approved prior to use.
7. Taking immediate action to resolve AIS security deficiencies.

Document Requirements

The SELLER shall be responsible for control of documents issued to them by the BUYER. Further issuance of documents to lower-tier subcontractors and/or suppliers does not relieve the SELLER of this responsibility.

- Document Classification

No BUYER or SELLER information associated with CNS is released without review and approval by BUYER (CNS Classification Office) for release restrictions. Only the BUYER or a BUYER-trained and certified individual will classify and mark documents. SELLER shall protect at the highest level marked on any documents contained in the Purchase Order Documents. Information should be marked as "**Protect as UCNI Pending Review"** and protected accordingly pending a classification review by a Derivative Classifier/UCNI Reviewing Official. When a document must be sent outside the originating organization for review, the document must be transmitted as described in detailed instructions of Appendix A.

- Reproduction
    1. Reproduction of UCNI/OUO information shall not be performed by the SELLER without prior approval of reproduction equipment by the BUYER and the UCNI/OUO Information Protection Team.

Transmission of UCNI/OUO Information

All transmission of UCNI/OUO matter shall be by means that preclude unauthorized disclosure or dissemination.

- Electronic Transmission of UCNI/OUO Information
    1. No transmissions via computer of UCNI/OUO information will be allowed unless formally pre-approved by the BUYER and UCNI/OUO Information Protection Team.
    2. Electronic media transmissions shall be encrypted using BUYER approved FIPS 140-2 Level 1 or higher encryption modules.
- Telephone Transmissions
    1. All voice transmissions of UCNI information shall be over BUYER approved secure telephone units or approved encrypted communication links. Applications utilized across Internet or distribution of sensitive information over Internet is not permitted unless through encryption (i.e., Entrust or CNS Cybersecurity approved encryption methods) and then only after certification by the CNS UCNI/OUO Information Protection Cybersecurity Lead.
    2. All voice transmissions of OUO information shall be made over physical landlines and shall not utilize cellular phone transmissions, or cordless phones.

- Fax Transmission of UCNI/OUO Information
  1. No fax transmissions of UCNI are allowed.
  2. Fax transmissions of OUO information should be protected by encryption when possible. Unencrypted fax transmissions are permissible only when :
     - It is preceded by a telephone call to the recipient so that he or she can control the document when it is received or respond to the sender that the facsimile was not received as expected, and
     - The sender is assured by the recipient that the facsimile is, and will be, only in the possession of an individual who has the proper need-to-know and is a U.S. citizen. Although not required, it is encouraged that the sender obtains a positive response from the recipient that the fax was received as expected.
- Document Transmission Within an Approved Facility
  1. A single opaque envelope, wrapper or coversheet may be used.
  2. Internal mail systems must use a sealed opaque envelope marked TO BE OPENED BY ADDRESSEE ONLY.
  3. An authorized individual may hand carry the matter as long as he/she can control access.
- Document Transmission Outside an Approved Facility
  1. Documents marked as UCNI or OUO shall be packaged in a single, opaque envelope or wrapping. The envelope shall be sealed and marked TO BE OPENED BY ADDRESSEE ONLY.
  2. Any of the following U.S. mail methods may be used:
     - First Class, Express, Certified, or Registered Mail.
     - Any commercial carrier using a signature service may be used.
  3. An authorized individual may hand carry the matter as long as he/she can control access.

Destruction of UNCI / OUO Information

UCNI/OUO documents generated as part of daily work that requires disposal may be destroyed using an approved cross-cut shredder that produces strips no more than ¼-inch wide and 2-inches long. Documents that cannot be destroyed using approved shredders (e.g., media, mylar, etc.) must be returned to the BUYER.

Return of UCNI / OUO Information for Destruction

A SELLER awarded a contract shall return UNCI/OUO electronic data and all media used to process UCNI/OUO information supplied by the BUYER or generated by the SELLER or lower-tier subcontractors and/or suppliers to the BUYER at the termination of the Purchase Order or upon termination of the certification of the computer. AIS equipment will be sanitized of all UCNI/OUO information by the BUYER before connecting to a network or computer system of a lower category or before equipment is removed from service. The SELLER and the BUYER will retain an accountability of media and contents. When lower-tier subcontractors and suppliers have completed their work, the associated data media and materials shall be forwarded to the SELLER. The SELLER will return all media involved in handling UCNI/OUO information to the BUYER for accountability and destruction. At the termination of the Purchase Order, the SELLER shall provide written notification to the BUYER stating all UCNI/OUO information was destroyed and/or returned to the BUYER.

Infractions and Incidents

Failure to comply with requirements specified herein may result in an Incident of Security Concern (IOSC). The SELLER is responsible for SELLER costs incurred because of IOSCs due to SELLER error. Any person who violates applicable civil law under Atomic Energy Act provisions is subject to civil penalties or may face criminal prosecution.

Notifications of security breaches or deviations from expectations shall be reported to the BUYER or Y-12 Plant Shift Superintendent (PSS) at 865-574-7172 or Pantex Operations Center at 806-477-5000. The SELLER shall cooperate with the Y-12 or Pantex Incident of Security Concerns (IOSC) organization in the conduct of an inquiry of an incident.

All computer security incidents involving UCNI/OUO information or AIS resources shall be reported immediately to the BUYER (or PSS/Pantex Operations Center), including:

1. Fraudulent action involving AIS.
2. Processing of information without an approved Security Plan.
3. Leaving a session active while not properly protected (e.g., unattended, unsupervised).
4. Unauthorized testing of an approved AIS.
5. Printer ribbons, cards, diskettes, hardcopy output, and/or magnetic media left unattended (not properly physically protected).
6. Disclosure of sensitive information (e.g., failure to protect data files properly).
7. Hackers/crackers or other unauthorized access attempts.
8. Using CNS UCNI/OUO information on unapproved/uncertified AIS.
9. Connecting certified AIS to an unapproved network.

Applicable Regulatory Requirements

1. 10 CFR 1017, Identification and Protection of Unclassified Controlled Nuclear Information
2. DOE O 471.1B, Identification and Protection Unclassified Controlled Nuclear Information
3. DOE O 471.3, Identifying and Protecting Official Use Only Information
4. DOE M 471.3-1, Manual for Identifying and Protecting Official Use Only
5. DOE G 471.3-1, Guide to Identifying Official Use Only Information
6. DOE O 205.1B, Department of Energy Cyber Security Program
7. NNSA SD 205.1, NNSA Baseline Cyber Security Program
8. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Applicable Procedures and Policies

1. Y19-401, Automated Information System (AIS) Security Handbook (OUO)
2. Y15-404, Acceptable Use of Information Technology Equipment
3. MVP09-00051-01, Unclassified Master Information System Security Plan (Unclassified-ISSP)(OUO)
4. Y30-205, Exporting Compliance for Foreign National Transactions: Commodities, Hardware, Software, and Information
5. CNS E-PROC 3123, Identification and Protection of UCNI and OUO Information
6. CNS CSPP, Cybersecurity Program Plan for the Pantex Plant and Y-12 National Security Complex

Appendix A

1. Purpose

This Appendix defines the requirements for the Identification and Protection of Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO) Information per the Department of Energy (DOE) Order 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, DOE Order 471.3, *Identifying and Protecting Official Use Only Information*, DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information,* 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information,* DOE Order 206.1, *Department of Energy Privacy Program and* NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. SELLER is responsible for complying with the Contractor Requirements Document (CRD) of these orders and flowing down the CRD requirements to the subcontractor(s) at all tiers, to the extent necessary to assure contractor compliance.

Note: Currently within the DOE and the National Nuclear Security Administration (NNSA), the term Controlled Unclassified Information (CUI) has dual meanings. One, it's an overarching term used to refer to unclassified information that is identified and marked as sensitive (e.g. UCNI and OUO to include Personally Identifiable Information [PII]). Secondly, the term is also used to describe information that will eventually be identified and safeguarded under 32 Code of Federal Regulations (CFR) 2002, which mandates a U.S. Government-wide uniform program to identify and protect sensitive, but unclassified information. However, 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. Therefore, the DOE Office of Classification has directed all contractor and federal employees to continue to identify and protect UCNI and OUO to include Personally Identifiable Information (PII) in accordance with already established DOE Orders and federal regulations. – DOE Office of Classification (AU-60), *Controlled Unclassified Information and Executive Order 13556*, https://www.energy.gov/ehss/controlled-unclassified-information-and-eo-13556

2. Applies To

This Appendix is applicable to all vendors/subcontractors and other personnel who conduct official business with the Y-12 National Security Complex and Pantex Plant. It is to be used when required to identify and protect UCNI and OUO Information shared with third party, non-federal personnel and entities.

3. Other Documents Needed

- UCN-22414, *Identification and Protection of UCNI/OUO Information*
- UCN-22435, *Certification as a United States Citizen in order to Handle UCNI/OUO*

4. References

- DOE O 471.1B, *Identification and Protection of 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 Information*
- 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 206.1, *Department of Energy Privacy Program*.

5. Roles and Responsibilities

5.1 CNS Classification Officer

1. Appointed and designated to administer the UCNI/OUO Information Protection Program at the Y-12 National Security Complex (NSC) and Pantex Plant.
    a. Serves as lead UCNI Reviewing Official (RO) for both sites.
    b. May delegate personnel to execute various aspects of UCNI/OUO administration in support of DOE O CRD information protection program action requirements.
2. Ensures CRD of DOE O 471.1B and 471.3, Admin Change 1, and 206.1 are flowed down to subcontractors at any tier, to extent necessary to ensure contractor compliance.
3. Every two (2) years at minimum, IAW DOE O 471.1B CRD, prepares written self-assessment of the implementation of the UCNI program requirements, including corrective action plans for any deficiencies noted.
4. At least once every five (5) years, reviews contract UCNI guidance, regardless of whether any revision or page changes have occurred.
5. Utilizes current UCNI guidance to develop detailed contract-level UCNI guidance, tailored to the needs of Pantex/Y-12 mission requirements, and ensures that guidance is revised when no longer current or complete.
6. Ensures any new or revised UCNI guidance is distributed to the appropriate UCNI ROs within 30 calendar days, and requires any superseded guidance be returned to the Classification Office for proper destruction.
7. Periodically evaluates vendor/subcontractor off-site facilities that handle or generate UCNI/OUO information.
8. Ensures any individual nominated to be an UCNI Reviewing Official (RO): 1) is competent in the subject areas in which their authority will be used; 2) familiar with DOE UCNI policy, procedures, and guidance; and 3) successfully completes initial training and recertification every two (2) years.

9. Ensures individuals with routine access to UCNI are briefed periodically through awareness briefings on their responsibilities for identifying and protecting UCNI.
10. Ensures any cover sheets used at either site for documents containing UCNI are approved by the cognizant security authority.
11. Guides development, approval and interpretation of policies and procedures for Pantex/Y-12 UCNI/OUO information protection in accordance with applicable DOE/NNSA directives.
12. Serves as the liaison between Contractor and the NNSA Production Office (NPO) for UCNI/OUO information protection matters.
13. Requests the necessary support and resources to ensure adequate administration and oversight of the contract UCNI/OUO Information Protection Program.

5.2 CNS Subcontract Procurement Representatives (BUYER)

1. Coordinates with the Subcontract Technical Representative (STR) and Subcontractor Company whenever procurement activities may involve UCNI/OUO information protection with the UCNI/OUO Information Protection Team (Enterprise Classification Office).
2. Employs UCN-26608, *UCNI/OUO Information Protection Requirements for CNS Suppliers* to ensure identification and protection requirements for UCNI/OUO information are addressed in procurement contracts.
3. Acts as a liaison between the Subcontractor Company and CNS on all UNCI/OUO information protection matters, as defined by the subcontract and UCN-26608.
    a. Notifies the Subcontractor Company: IF they will be handling and generating UCNI/OUO Information, THEN it is strongly encouraged they coordinate with the Enterprise Classification Office to have personnel handling UCNI/OUO obtain UCNI/OUO information protection awareness training, and specific staff be certified as DOE UCNI ROs.
4. Employs UCN-22435 to establish that the vendor/subcontract company representative is a U.S. Citizen with a need to know prior to granting them access to UCNI.
5. Notifies the CNS UCNI/OUO Information Protection and CNS Cybersecurity Teams when an off-site facility is going to be generating UCNI/OUO information and/or Government Furnished Equipment (GFE) Laptop is provided to an off-site facility.

5.3 Subcontract Technical Representative (STR) Assigned to Subcontractor Company

1. Acts as a liaison between the Subcontractor Company and CNS on all UNCI/OUO information protection matters as defined by the subcontract.
2. Employs UCN-26608 to ensure subcontractors and potential contractors that access, use, or generate UCNI/OUO information:

a. Receive and understand the appropriate training prior to having access to UCNI/OUO information in accordance with UCN-26608.

b. Know and understand the requirements for protecting, marking, and transmitting UCNI/OUO information.

c. Comply with the contract-based classification, Identification and Protections requirements.

3. Ensures that the appropriate language for protecting UCNI/OUO information is a part of a Subcontractor Company's Statement of Work (SOW) and eventual subcontract.

4. Brings any concerns of potential UCNI/OUO mishandling to the immediate attention of the Procurement Representative and the Classification Office.

5. Ensures all UCNI/OUO information is retrieved from the subcontract company when no longer contractually required, or a statement of destruction is obtained from the subcontract company.

5.4 Subcontract Companies

1. Employs UCN-26608 to:

a. Identify/Appoint an UCNI/OUO Information Protection Point of Contact (POC) and Computer Security POC to coordinate and interface with the CNS UCNI/OUO Information Protection and CNS Cybersecurity Teams, and ensure the necessary physical security and cybersecurity measures are in place in order to properly protect unauthorized access to UCNI/OUO information.

b. Ensure contract provisions regarding the protection of UCNI/OUO in accordance with laws and applicable rules are effectively accomplished.

c. Provide oversight of all subcontractor employees and ensure compliance with UCNI/OUO Information Protection Program requirements.

d. Ensure all UCNI/OUO information is reviewed by a DOE trained ROs and protected at the appropriate level, as necessary.

e. Determine appropriate need-to-know for all subcontract employees in accordance with specific UCNI/OUO information protection requirements.

2. Maintains all records regarding the protection of UCNI/OUO required by the subcontract.

3. Ensures that those working on CNS projects know the identity of, and how to contact their CNS Subcontract Procurement Representative (Buyer) and STR.

4. Ensures all UCNI/OUO information/media is returned to the Buyer and STR when no longer contractually required, or properly destroyed with a statement of destruction provided.

5. If a trained UCNI Reviewing Official (RO) is on staff, then all employees handling UCNI/OUO information must know the identity of and how to contact the UCNI RO, in order to coordinate reviews of documents generated by the company.

    a. Subcontractor Companies who generate UCNI information are strongly encouraged to have trained UCNI ROs on staff. Training may be provided upon request by contacting the Classification Office.

Note: It's strongly encouraged that off-site facilities who generate UCNI information have a trained UCNI RO on staff. This training can be provided by contacting the CNS Classification Office.

6. Unclassified Controlled Nuclear Information

6.1 Review of a Document or Material for UCNI

1. UCNI is information concerning nuclear facilities, materials, weapons, and components whose dissemination is controlled under Section 148 of the Atomic Energy Act and 10 CFR 1017.

6.2 UCNI Review Process

1. Reviewing documents for UCNI - Anyone who originates or possesses a document that he or she thinks may contain UCNI must have a trained RO review for a determination before it is finalized, sent outside of his or her organization, or filed.
2. If the originator or possessor must send the document outside of his or her organization for the review, he/she must mark the front of the document with **''Protect as UCNI Pending Review''** and must transmit the document in accordance with the "Physical Protection Requirements of UCNI" listed below. Use a separate piece of paper on the first and last page of the document marked **PROTECT AS UCNI PENDING REVIEW** or an UCNI cover sheet may be used as the first page and last page of the document.
3. Organization is defined as the company (i.e., vendor, subcontractor) and the project staff (i.e., Y-12, Pantex, and Uranium Processing Facility). In cases where the vendor/subcontractor has a lower-tier they are collaborating with, the vendor/subcontractor serves as the project staff and the company serves as the lower-tier. When documents are transmitted between companies within the organization, they must be appropriately marked and protected. Documents that may contain UCNI, were created from an UCNI source, or are generated on UCNI certified and accredited equipment must bear the "Protect as UCNI Pending Review" stamp when transferred between companies within the organization.
4. The RO must first determine whether the document is widely disseminated in the public domain, which means that the document under review is publicly available from a Government technical information service or depository library, for example, or that it can be found in a public library or an open literature source, or it can be accessed on the Internet using readily available search methods.

5. If the document is determined to be widely disseminated in the public domain, it cannot be controlled as UCNI. The RO returns the document to the person who sent it to the RO and informs him or her why the document cannot be controlled as UCNI. This does not preclude control of the same information as UCNI if it is contained in another document that is not widely disseminated.
6. If the document is not determined to be widely disseminated in the public domain, the RO evaluates the information in the document using guidance to determine whether the document contains UCNI.
7. If the RO determines that the document does contain UCNI, the RO marks or authorizes the marking of the document as specified in "Marking UCNI Documents" below. If the RO determines that the document does not contain UCNI, the RO returns the document to the person who sent it and informs him or her that the document does not contain UCNI.
8. For documentation purposes, the RO may mark or authorize the marking of the document as specified in "Determining that a document or material no longer contains or does not contain UCNI" below.

6.3 Review Exemption for UCNI Documents in Files

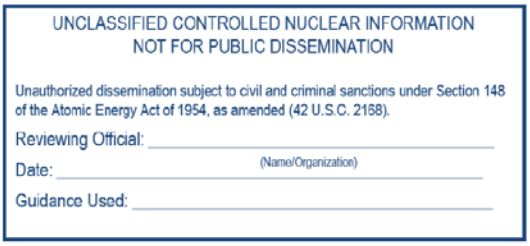
1. Any document that was permanently filed prior to May 22, 1985, is not required to be reviewed for UCNI while in the files or when retrieved from the files for reference, inventory, or similar purposes as long as the document will be returned to the files and is not accessible by individuals who are not Authorized Individuals for the UCNI contained in the document.
2. IF a document that is likely to contain UCNI is removed from the files for dissemination within or outside of the immediate organization, THEN it must be reviewed by a RO with cognizance over the information.

6.4 UCNI Markings on Documents or Material

Note: DO NOT USE the marking ''May Contain UCNI''. This marking is no longer authorized for use. If a legacy document is marked ''May Contain UCNI'' it is considered to contain UCNI and must be protected accordingly until a RO or Denying Official determines otherwise.

1. Marking UCNI Documents: If a RO determines that a document contains UCNI, the RO must mark or authorize the marking of the document as described:

   The following marking must appear on the front of the document:


UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
NOT FOR PUBLIC DISSEMINATION

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: _____
(Name/Organization)

Date: _____

Guidance Used: _____

2. Marking Pages: The marking ‘‘Unclassified Controlled Nuclear Information’’ must be placed on the bottom of the front of the document and on the bottom of each interior page of the document that contains text or if more convenient, on the bottom of only those interior pages that contain UCNI.

   The page marking must also be placed on the back of the last page. If space limitations do not allow for use of the full-page marking, the acronym ‘‘UCNI’’ may be used as the page marking.

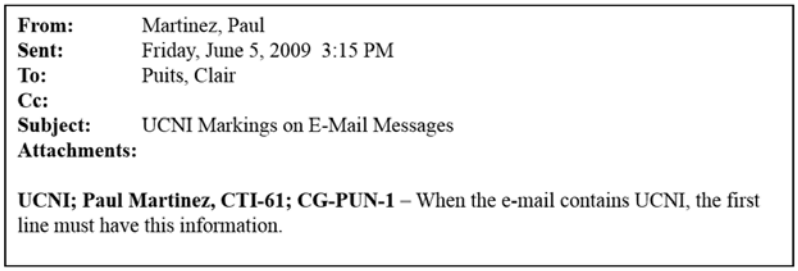
   Note 1: UCNI markings must be applied to any unclassified document or material that contains or reveals UCNI regardless of any other unclassified control marking (e.g., OUO) that is also on the document or material.

   Note 2: A title or subject should not contain the acronym UCNI unless unavoidable. If unavoidable, the acronym “UCNI” must be placed at the end of the title or subject.

3. Marking UCNI Material: If possible, material containing or revealing UCNI must be marked as described above. If space limitations do not allow for use of the full marking, the acronym ‘‘UCNI’’ may be used.

4. Special Format Documents or Material: Standard markings must be applied to unclassified documents in special formats (e.g. photographs, viewgraphs, films, magnetic tapes, disks, flash memory drives, audio or videotapes, slides) or material to the extent practical. Regardless of the precise markings in such cases, any special-format unclassified document or material that contains UCNI must be marked so that both a person in physical possession of the document or material and a person with access to the information in or on the document or material are made aware that it contains UCNI. For example, a compact disk must be marked both on the disk and on the container and the appropriate electronic files on the disk must also be marked.

5. Marking UCNI Emails: The first line of an e-mail message containing UCNI must include the abbreviation “UCNI,” the RO’s name and organization, and the guidance used to make the UCNI determination. See example below:



From: Martinez, Paul
Sent: Friday, June 5, 2009 3:15 PM
To: Puits, Clair
Cc:
Subject: UCNI Markings on E-Mail Messages
Attachments:

UCNI; Paul Martinez, CTI-61; CG-PUN-1 – When the e-mail contains UCNI, the first line must have this information.

Note: If the individual drafting the UCNI email is not a trained UCNI RO, the email must be reviewed by an UCNI RO and contain their information as outlined above prior to being sent. As a best practice this admonishment should then be repeated by each additional author as the email is replied to or forwarded on, keeping the admonishment at the top of the email chain.

6. Emails with UCNI Attachments: If there is an attachment that contains UCNI, it must have all required UCNI markings. If the message itself is not UCNI but an attachment contains UCNI, the message must indicate that the attachment is UCNI (Example: ***"Attachments contain UNCLASSIFIED CONTROLLED NUCLEAR INFORMATON. When separated from attachments, this email is Unclassified and contains no UCNI"***). The attachment must have all required UCNI markings.
7. Transmittal Documents: A document that transmits documents or material marked as containing UCNI and does not itself contain classified information or UCNI must be marked on the front of the document as indicated below. If the transmittal document does not itself contain UCNI, no UCNI markings should be placed on the transmittal document.

> Document(s) transmitted contain(s)
> Unclassified Controlled Nuclear Information.
> When separated from enclosures, this
> transmittal document does not contain UCNI

6.5 Determining that a Document or Material no Longer Contains or Does not Contain UCNI

A RO with cognizance over the information in a document or material marked as containing UCNI may determine that the document or material no longer contains UCNI. The official making this determination must base it on applicable guidance and must ensure that any UCNI markings are crossed out (for documents) or removed (for material). The official marks or authorizes the marking of the document (or the material, if space allows) as follows:

> DOES NOT CONTAIN
> UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
> Reviewing/Denying Official: Michael Kieszkowski, CTI-61
> (Name/Organization)
> Date: 4/30/16

6.6 Access to UCNI

1. Need to Know: In addition to the specific requirements listed in this procedure, all individuals granted access to UCNI must be trained and meet need-to-know criteria in accordance with 10 CFR 1017. Need to know means a determination made by an Authorized Individual that a person requires access to specific UCNI to perform official duties or other Government-authorized activities. Curiosity, being a supervisor of an individual, or being an owner of a company does not constitute a need-to-know.
2. Access limitations: An individual may only have access to UCNI if he or she has been granted routine access by an Authorized Individual or limited access by the DOE Program Secretarial Officer or NNSA Deputy or Associate Administrator with cognizance over the UCNI (In accordance with 1017.21 of 10 CFR 1017). The

Secretary, or his or her designee, may impose additional administrative controls concerning the granting of routine or limited access to UCNI to a person who is not a U.S. citizen.

Note: An individual who is in possession of UCNI and grants routine access to another person must notify each individual granted such access of the applicable handling requirements.

3. Routine Access:

   a. Authorized Individual - The RO who determines that a document or material contains UCNI is the initial Authorized Individual for that document or material. An Authorized Individual, for UCNI in his or her possession or control, may determine that another person is an Authorized Individual who may be granted access to the UCNI, subject to limitations in paragraph (b) of this section, and who may further disseminate the UCNI under the provisions of this section.

   b. Requirements for routine access - To be eligible for routine access to UCNI, the individual must have a need to know the UCNI in order to perform official duties or other Government-authorized activities and must be a U.S. citizen who is: 1. An employee of any branch of the Federal Government, including the U.S. Armed Forces; 2. An employee or representative of a State, local, or Indian tribal government; 3. A member of an emergency response organization; 4. An employee of a Government contractor or a consultant, including those contractors or consultants who need access to bid on a Government contract; 5. A member of Congress or a staff member of a congressional committee or of an individual member of Congress; 6. A Governor of a State, his or her designated representative, or a State government official; 7. A member of a DOE advisory committee; or, 8. A member of an entity that has entered into a formal agreement with the Government, such as a Cooperative Research and Development Agreement or similar arrangement; or, A person who is not a U.S. citizen but who is: A Federal Government employee or a member of the U.S. Armed Forces; An employee of a Federal Government contractor or subcontractor; A Federal Government consultant; A member of a DOE advisory committee; A member of an entity that has entered into a formal agreement with the Government, such as a Cooperative Research and Development Agreement or similar arrangement; An employee or representative of a State, local, or Indian tribal government; or, A member of an emergency response organization when responding to an emergency; or, A person who is not a U.S. citizen but who needs to know the UCNI in conjunction with an activity approved by the DOE Program Secretarial Officer or NNSA Deputy or Associate Administrator with cognizance over the UCNI.

      Note: For NNSA sites, this authority is the NNSA Associate Administrator for Defense Nuclear Security (NA-70).

4. Limited Access: An individual who is not eligible for routine access to specific UCNI under 1017.20 may request limited access to such UCNI by sending a written request to the DOE Program Secretarial Officer or NNSA Deputy or Associate Administrator with cognizance over the information. A person granted limited access to specific UCNI is not an Authorized Individual and may not further disseminate the UCNI to anyone.

   Note: For NNSA sites, this authority is the NNSA Associate Administrator for Defense Nuclear Security (NA-70).

6.7 Physical Protection Requirements of UCNI

1. Notification of protection requirements: An Authorized Individual who grants routine access to specific UCNI to an individual who is not an employee or contractor of the DOE must notify the person receiving the UCNI of protection requirements described in this manual and in accordance Subpart E – Physical Protection Requirements of 10 CFR 1017 and any limitations on further dissemination.
2. Protection in use: An Authorized Individual or a person granted limited access to UCNI must maintain physical control over any document or material marked as containing UCNI that is in use to prevent unauthorized access to it.
3. Storage: A document or material marked as containing UCNI must be stored to preclude unauthorized disclosure. When not in use, documents or material containing UCNI must be stored in locked receptacles (e.g., file cabinet, desk drawer), or if in secured areas or facilities, in a manner that would prevent inadvertent access by an unauthorized individual.
4. Reproduction: A document marked as containing UCNI may be reproduced without the permission of the originator to the minimum extent necessary consistent with the need to carry out official duties, provided the reproduced document is marked and protected in the same manner as the original document. All reproduction equipment requires certification and accreditation by CNS Cybersecurity.
5. Destruction: A shredder must be a cross-cut shredder that produces particles no larger than 1/4 –inch wide and 2 inches long, and it must be checked after every use for compliance.
6. Transmission: Physically transmitting UCNI documents or material. A document or material marked as containing UCNI may be transmitted by: 1. U.S. First Class, Express, Certified, or Registered mail; 2. Any means approved for transmission of classified documents or material; 3. An **Authorized Individual** or person granted **limited access** under 6.6.4 of this procedure as long as physical control of the package is maintained; or, 4. Internal mail services.

   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.’’

7. Telecommunication Circuits: When Transmitting UCNI documents over telecommunications circuits encryption algorithms will be used that comply with all applicable Federal laws, regulations, and standards for the protection of CUI must be used. This includes all telephone, facsimile, radio, e-mail, and Internet communications.

   At Pantex: The Pantex telephone systems and communications lines are authorized for the transmission of UCNI under specific conditions and only in accordance with the architecture, protections, and use case specifically denoted within an exception granted by NNSA; specifically, UCNI telephone conversations are only allowed between phones on the Pantex telephone system (i.e., internal communications). Personnel can identify internal phone numbers by the local area code and prefix of 806.573-XXXX or within the range of 806.477.3000 to 806.477.7999. UCNI telephone conversations or faxes from the Pantex telephone system to any number external to the Pantex telephone system is prohibited.

   At Y-12: The Y-12 telephone system and communications lines are not authorized for the transmission of UCNI; as such, both telephone conversations and faxes of UCNI are prohibited on the Y-12 telephone system. A Secure Terminal Equipment, OMNI secure phone or VIPeR phone must be used for both telephonic conversations and faxing of UCNI.

8. Processing on Automated Information Systems (AIS): UCNI may be processed or produced on any AIS that complies with the guidance in the Office of Management and Budget (OMB) Circular No. A–130, Revised, Transmittal No. 4, Appendix III, ‘‘Security of Federal Automated Information Resources,’’ is secured in accordance with NIST SP 800-171 and approved by CNS Cybersecurity approved by CNS Cybersecurity, or is certified for classified information.

   Note: All UCNI E-mail messages sent between ***cns.doe.gov*** and ***npo.doe.gov*** use a Virtual Private Network (VPN) encryption algorithm, which ensures e-mail traffic is fully encrypted, and additional software encryption (i.e., Entrust) is not required when sending UCNI e-mail message between these two addresses. However, if you send a message containing UCNI to any email address other than these two, you must encrypt it before it is sent outside the CNS Border Network.

9. UCNI Cover Sheets: Use of a cover sheet for documents containing UCNI is not required. However, the custodian of an UCNI document is responsible for ensuring that the recipient is knowledgeable of UCNI requirements and an UCNI cover sheet attached to the front of the document is a fast and cost-effective method of meeting this requirement.

At Pantex:
Gold in color, titled; ***"UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI) NOT FOR PUBLIC DISSEMINATION"***

At Y-12:
Green in color, titled;
"UCNI COVER SHEET"

6.8 Violations

1. Civil Penalty: Any individual who violates a UCNI security requirement of any of the following is subject to a civil penalty under 10 CFR Part 1017—Identification and Protection of Unclassified Controlled Nuclear Information; or any other DOE regulation related to the safeguarding or security of UCNI if the regulation provides that violation of its provisions may result in a civil penalty pursuant to section 148 of the Act.
2. Criminal Penalty: Any individual who violates section 148 of the Atomic Energy Act or any regulation or order of the Secretary issued under section 148 of the Atomic Energy Act, including these regulations, may be subject to a criminal penalty under section 223 of the Atomic Energy Act (42 U.S.C. 2273). In such case, the Secretary shall refer the matter to the Attorney General for investigation and possible prosecution.

7. Official Use Only (OUO) Information

7.1 Identifying and Marking OUO Information

Note 1: Except for UCNI and Naval Nuclear Propulsion Information, OUO markings are the only markings to be used to designate documents. Additional markings that are based on law, regulation, or other DOE CRD that convey additional advice on handling or access restrictions (e.g., "Protected Cooperative Research and Development Agreement (CRADA) Information," "Export Controlled Information") are allowed.

Note 2: OUO information is information that has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not have a need to know the information to perform their jobs or other DOE-authorized activities, and falls under at least one of the eight Freedom of Information Act (FOIA) exemptions.

To be identified as OUO, information must be unclassified and meet both of the following criteria:

1. Have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or

other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.

2. Fall under at least one of eight FOIA exemptions (exemptions 2 through 9; information falling under exemption 1 can never be OUO because it covers information classified by Executive Order). These exemptions describe types of information whose unauthorized dissemination could damage governmental, commercial, or private interests.

An unclassified document that is originated within a DOE/NNSA office, produced by or for that office, or under the control of that office may contain OUO information. Any employee from an office with cognizance over such information may determine whether such a document contains OUO information. The process is as follows:

1. The employee first considers whether the information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities.
2. If the information is considered to have the potential for such damage, then the employee consults guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3. If the specific information in question is identified as OUO information in such guidance, then the employee determines that the document contains OUO information.
3. If the information is considered to have the potential for such damage, but no guidance issued under paragraphs 5a(3), 5a(4), or 5b(2) of DOE O 471.3 covers the specific information in question, then the employee considers whether the information falls under at least one of FOIA exemptions 3 through 9. If the employee believes that the information falls under one of the FOIA exemptions, then the employee may determine that the document contains OUO information.
4. If the employee finds no basis for identifying the information as OUO in guidance issued under DOE O 471.3 and does not believe the information falls under one of the FOIA exemptions, then the employee must not mark the document as containing OUO information.

7.2 Marking a Document that Contains OUO Information

1. Front Marking: The front marking must include the applicable FOIA exemption number and related category name, and the name and organization of the employee making the determination and the guidance used.

   FOIA Exemptions – **IN USE at CNS**

   Exemption 3 – 'Statutory Exemption' (Used when ECI is identified-*See Section 9*)

   Exemption 4 – 'Commercial/Proprietary'

   Exemption 5 – 'Privileged Information'

Exemption 6 – 'Personal Privacy'

Exemption 7 – 'Law Enforcement'

FOIA Exemptions **NOT IN USE at CNS** (not applicable, no longer in use, not used)

Exemption 1 – (**Not Applicable**) 'National Security Information'

Note: Information falling under exemption 1 can never be OUO because it covers information classified by Executive Order.

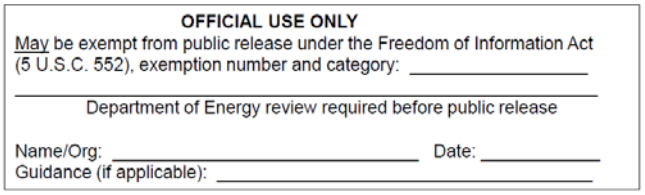
Exemption 2 – (**Not Used** at Pantex or Y-12) 'Circumvention of Statute'

***Note to RO:* IF you are tasked to review a document with Exemption 2 markings:** *Exemption 2 is no longer used. Per DOE, legacy documents in storage bearing Exemption 2 markings do not have to be changed. However, IF a document bearing Exemption 2 is removed from storage for the purpose of dissemination within/outside of the immediate organization, or content is derived from it in creation of a new document, THEN it must be reviewed by an RO with cognizance over the information, and remarked using Exemption 7, Law Enforcement.*

Exemption 8 – (**Not Used** at Pantex or Y-12) 'Financial Institutions'

Exemption 9 – (**Not Used** at Pantex or Y-12) **'**Wells'

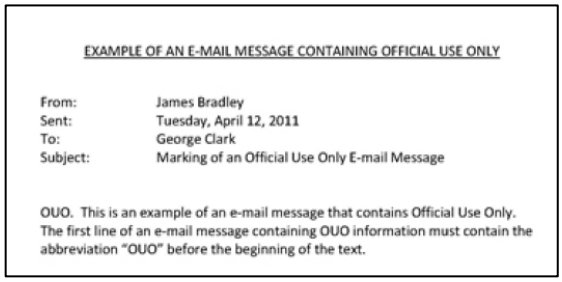
The employee making the determination ensures that the following marking is placed on the front of each document containing OUO information.



Note: Except for UCNI, which is identified, marked, and protected IAW 10 CFR 1017, and DOE O 471.1, and Naval Nuclear Propulsion Information which is controlled under 32 CFR 250, OUO markings are the only markings to be used within DOE to designate documents containing unclassified controlled information. Additional markings that are based on law, regulation, or other DOE directives that convey additional advice on handling or access restrictions (e.g., Source Selection Information-See Federal Acquisition Regulation 2-101 and 3.104; Protected CRADA Information; Export Controlled Information) are allowed.

2. Page Marking: The employee making the determination must ensure that the words "Official Use Only" (or "OUO" if space is limited) are placed on the bottom of each page or, if more convenient, on just those pages containing the OUO information.

3. Marking E-mail Messages: The first line of an e-mail message containing OUO information must contain the abbreviation "OUO" before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate that the attachment is OUO. The attachment must have all required OUO markings.



EXAMPLE OF AN E-MAIL MESSAGE CONTAINING OFFICIAL USE ONLY

From: James Bradley
Sent: Tuesday, April 12, 2011
To: George Clark
Subject: Marking of an Official Use Only E-mail Message

OUO. This is an example of an e-mail message that contains Official Use Only. The first line of an e-mail message containing OUO information must contain the abbreviation "OUO" before the beginning of the text.

Note: As a best practice the first line message of "OUO" should then be repeated by each additional author as the email is forwarded on, keeping the abbreviation at the top of the email chain.

4. Marking Special Format Documents: Special format documents (e.g., photographs, viewgraphs, films, magnetic tapes, floppy diskettes, audiotapes, videotapes, DVDs, or CD-ROMs) must be marked in a manner consistent with paragraphs 1 and 2 above so persons possessing the documents and persons with access to the information in or on the documents are aware that they contain OUO information. When space is limited, as on the frame of a 35-mm slide, the page marking is sufficient.

5. Marking Documents Maintained in Restricted Access Files: Documents that may contain OUO information that are maintained in files to which access is restricted (e.g., personnel office files) do not need to be reviewed and marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized access to the OUO information. However, a document removed from these files and not to be returned (or a copy of such document) must be reviewed to determine whether it contains OUO information and, if appropriate, marked.

Note: Documents that are moved from one restricted access file location to another for storage purposes do not need to be reviewed.) Documents that are removed for criminal, civil, or administrative law enforcement or prosecution purposes need not be reviewed or marked where parallel

6. Transmittal Document: A document that transmits an attachment or enclosure marked as containing OUO information and does not itself contain classified or controlled information must be marked on its front as indicated below to call attention to the presence of OUO information in the attachments or enclosures. If the transmittal document does not itself contain UCNI or OUO, no UCNI or OUO markings should be placed on the transmittal document.

Document transmitted
contains OUO information

7.3 Removal of OUO Markings

Note: For removal of OUO-Export Controlled Information (ECI) markings consult the Export Office.

1. Markings Applied Based on Guidance:

   OUO markings applied based on guidance may be removed by any employee when the guidance used to make the determination states that the information is no longer OUO. (For example, a topic may state that unclassified information that describes certain deficiencies at a site/facility/security area that have not been corrected is OUO. Once those deficiencies have been corrected, the OUO marking may be removed.)

2. Markings Applied Based on Employee's Evaluation: OUO markings applied based on an employee's evaluation may be removed by (1) the employee who initially applied the marking, (2) the supervisor of the employee who initially applied the marking, or (3) a FOIA authorizing official who approves the release of the document in response to a request made under FOIA.

   Whoever makes the determination to remove the markings ensures that the markings are crossed out or otherwise obliterated and places the following marking on the bottom of the front of the document:

DOES NOT CONTAIN
OFFICIAL USE ONLY INFORMATION
Name/Org: Michael Kieszkowski, IM-40 Date: 4/30/14

7.4 Relationship of OUO Markings to Other Types of Control Markings

1. Unclassified Documents: The OUO front marking must be applied to any unclassified document that contains OUO information regardless of any other unclassified control marking (e.g., UCNI).

2. Classified Documents: OUO front and page markings must not be applied to any classified document that also contains OUO information. However, if the classified document has been portion marked, the acronym "OUO" must be used to indicate those portions containing only OUO information.

3. Marking Documents Generated Before April 9, 2003: Unclassified documents generated before April 9, 2003 are not required to be reviewed to determine whether they contain OUO information unless they are to be publicly released. Any such previously generated document determined to contain OUO information after April 9, 2003 must be marked as indicated in Section 7.2 above. Such determination may be made by anyone in the organization that currently has cognizance over the information in the document. In addition, for unclassified

documents marked as containing OUO information before the date of this Manual, the markings are not required to be updated to conform to the marking requirements in this Manual.

4. Obsolete Markings: From July 18, 1949, to October 22, 1951, the Atomic Energy Commission used the term "Official Use Only" as a designation for certain classified information. Documents from this time period with an OUO marking must be handled as Confidential National Security Information pending a determination of their proper classification.

5. Equivalent Markings: Ensure that documents marked as containing OUO information and other-Agency documents with equivalent markings [e.g., For Official Use Only from the Department of Defense; Sensitive but Unclassified (SBU) from the Department of State; Limited Official Use from the Department of Justice] are protected in accordance with 7.5 thru 7.7 of this procedure.

7.5 Protecting OUO Information

1. Access to OUO Information: Access to a document(s) marked as containing OUO information and OUO information from such documents must only be provided to those individuals who require the information to perform their jobs or other DOE-authorized activities. The responsibility for determining whether someone has a valid need for such access rests with the person who has authorized possession, knowledge, or control of the information or document and not on the prospective individual recipient.

7.6 Physical Protection Requirements for OUO

Note: Ensure that documents marked as containing OUO information and other-Agency documents with equivalent markings [e.g., "For Official Use Only" from the Department of Defense; SBU from the Department of State; "Limited Official Use" from the Department of Justice] are protected in accordance with these requirements.

1. Protection in Use: Reasonable precautions must be taken to prevent access to documents marked as containing OUO information by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don't read an OUO document in a public place, such as a cafeteria, on public transportation).

2. Protection in Storage: Documents marked as containing OUO information may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during non-duty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).

3. Reproduction: Documents marked as containing OUO information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO information. All reproduction equipment requires certification and accreditation by CNS Cybersecurity. Excess paper containing OUO information must be destroyed as described below.
4. Destruction: A shredder must be a cross-cut shredder that produces particles no larger than 1/4 –inch wide and 2 inches long, and it must be checked after every use for compliance.
5. Transmission:
    a. By Mail—Outside of a Facility:
        - Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY."
        - Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail.
        - Any commercial carrier may be used.
    b. By Mail—Within a Facility: Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.
    c. By Hand—Between Facilities or Within a Facility: A document marked as containing OUO information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.
    d. Over Telecommunications Circuits: When Transmitting OUO documents over telecommunications circuits encryption algorithms should be used that comply with all applicable Federal laws, regulations, and standards for the protection of CUI whenever possible. This includes all telephone, facsimile, radio, e-mail, and Internet communications. However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.
    e. By Unencrypted Facsimile: An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.
    f. By E-mail without Encryption: If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.

g. Transmission over Voice Circuits: OUO information transmitted over voice circuits should be protected by encryption whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits (minus cellular phones) may be used.

7.7 Violations

An administrative penalty may be imposed, as appropriate, if:

- OUO information from a document marked as containing OUO information is intentionally released to a person who does not need to know the information to perform his or her job or other DOE-authorized activities,
- A document marked as containing OUO information is intentionally or negligently released to a person who does not need to know the information to perform his or her job or other DOE-authorized activities,
- A document that is known to contain OUO information is intentionally not marked, or
- A document that is known to not contain OUO information is intentionally marked as containing such information.

8. Personally Identifiable Information – Official Use Only Exemption 6

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

High Risk PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of High Risk PII include, Social Security Numbers (SSNs), biometric records (e.g. fingerprints, Deoxyribonucleic Acid [DNA], etc.) health and medical information, and financial information (e.g. credit card numbers, credit reports, bank account numbers, etc.).

While all PII must be handled and protected appropriately, High Risk PII must be given greater protection and consideration following a breach because of the increased risk of harm to an individual if it is misused or compromised.

In some cases PII overlaps Privacy Act Information. All information of this nature is categorized as OUO Exemption 6, Personal Privacy, and should not be removed from DOE facilities without the written authorization of the employee or the employee's supervisor.

8.1 Examples of what is PII

1. SSNs, including abbreviated SSNs that utilize only the last four digits, are considered PII
2. Place of birth associated to an individual
3. Date of birth associated with an individual

4. Mother's maiden name associated with an individual
5. Biometric record associated with an individual
    a. Fingerprint
    b. Iris scan
    c. DNA
6. Medical history information associated with an individual
    a. Previous diseases
    b. Metric information
    c. Weight
    d. Height
    e. Blood Pressure
7. Criminal history associated with an individual
8. Employment history associated with an individual. Performance elements and standards (or work expectations) are PII when they are so intertwined with performance appraisals that their disclosure would reveal an individual's performance appraisal:
    a. Ratings
    b. Disciplinary actions
9. Financial information associated with an individual
    a. Credit card numbers
    b. Bank account numbers
10. Security clearance history or related info (not including actual clearances held)

8.2 Examples of what is Not PII

1. Phone numbers (work, home, cell)
2. Street addresses (home, work, other)
3. E-mail addresses (work or personal)
4. Digital pictures
5. Birthday cards
6. Birthday e-mails
7. Present and past grade and step information
8. Medical information pertaining to work status (X is out sick today)
9. Medical information included in a health or safety report (X broke his arm when...)
10. Resumes unless it includes SSN
11. Job titles for employment history, resume, or written biography

12. Present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, meritorious or distinguished executive ranks, and allowances and differentials)
13. Present and past position titles and occupational series
14. Position descriptions
15. Written biographies (like the ones used in pamphlets of speakers)
16. Alma mater or degree level
17. Personal information stored by individuals on their personal workstation or laptop (unless a SSN)

8.3 Protection of PII

Documents containing PII must be stored in a manner that applies strict need-to-know criteria. Under no circumstances should PII be accessible to unauthorized individuals. Storage of PII on local electronic storage media, including desktop and laptop hard drives and all removable media, should be reduced to the minimum necessary level and must be encrypted. Unnecessary PII files should be deleted. PII data should be relocated to internal network-based storage whenever possible.

Under no circumstances should PII other than for oneself be stored on a private computer or personally owned electronic storage media.

A Privacy Impact Assessment (PIA) is required for unclassified information systems per DOE O 206.1, *Department of Energy Privacy Program*. For any information system that will contain (collect and/or maintain), or plan to contain any information about individuals, a full PIA is required. Unclassified information system owners must perform a PIA prior to submitting a security plan for initial accreditation for production use. Owners of existing systems containing information about individuals who did not perform a PIA by April 30, 2010, must perform a PIA prior to submitting a security plan for re-accreditation.

The collection and use of Social Security numbers not required by statute, regulation or an intended DOE/NNSA purpose is prohibited in future information systems and software applications, and shall be eliminated where they are presently used as soon as practical, but prior to submitting a security plan for initial or reaccreditation, or prior to application software certification for production use.

8.4 Requirement for Reporting Compromised or Potentially Compromised PII

Any incident involving the suspected or confirmed compromise (i.e., unauthorized release) of PII, must be reported to the Y-12 Operations Center (OC) [formerly known as Plant Shift Superintendent's (PSS) Office] (865.574.7172) or the Pantex Operations Center (806.477.5000) immediately upon discovery (i.e., within 10 minutes of discovering the incident). Refer to E-PROC-3123 for additional details.

8.5 Privacy Act Information

The Privacy Act of 1974 (5 U.S.C. Sect 552(a)) requires the protection of certain types of information maintained on individuals.

The types of data that are protected by the Privacy Act include, but are not limited to:

- Promotions
- Disciplinary actions
- Appraisal and development records
- Payroll and leave records
- Reports of financial interest
- Supervisor maintained personnel records
- Personnel medical information
- Equal opportunity complaints
- Labor standards complaints and grievances
- Personnel security files
- Security investigations
- Personnel records of former contract employees, and
- Emergency locator records.

8.6 Violations

DOE and contractor employees who handle records must adhere to rules of conduct and ensure administrative, technical, and physical safeguards are in place to protect information from unwarranted disclosure or access by unauthorized persons. Penalties of up to $5,000 per incident are imposed on individuals who violate certain sections of the law, such as willfully and knowingly obtaining privacy information under false pretenses or willfully and knowingly disclosing privacy information unlawfully to third parties without the consent of the individual.

9. Export Controlled Information - Official Use Only (FOIA Exemption 3)

Note: See the Export Compliance webpage for more information on ECI.

An Export Controlled document may contain:

1. Unclassified information that reveals technological information that would aide someone in the development, production, or use of a technology or commodity; that has not been released readily in the public domain; and is not intended for public release by the sponsor; or

2. Information relating to military end-use technology, missile or satellite technology, nuclear reactor or special nuclear material technology, or nuclear/chemical/biological weapons, sensor technology, or explosives technology.

All ECI (Export Controlled documents) must be marked appropriately as OUO, exemption 3, Statutory Exemption, and should be marked in accordance with this procedure. **Unless specifically authorized by the Export Compliance Office foreign nationals are not allowed access to ECI.** All information thought to contain ECI must be reviewed for ECI. The CNS Export Compliance Office has final determination authority.
Particularly susceptible areas for ECI at CNS are Emerging Technologies or New Initiatives:

- Highly Enriched Uranium Materials Facility
- Special Materials Complex
- Uranium Production Facility
- Weapon Production Technologies
- Capacity and Utilization
- Explosives Technologies

Following is a list of the Federal Export Control Regulations that particularly apply to CNS:

Assistance to Foreign Atomic Energy Activities, DOE (10 CFR 810): Technology controls applies to activities involving nuclear reactors and other nuclear fuel cycle facilities for the following fluoride and nitrate conversion; isotope separation (enrichment); the chemical, physical or metallurgical processing, fabricating or alloying of special nuclear material; production of heavy water, zirconium (hafnium-free or low-hafnium), nuclear-grade graphite or reactor-grade beryllium; production of reactor-grade uranium dioxide from yellowcake; and certain uranium milling activities.

Nuclear Regulatory Commission (10 CFR 110): Materials include Special Nuclear Materials, Source Material, Byproduct Material, Deuterium, Nuclear grade graphite for nuclear end use, Production and utilization facilities. Equipment controls include Nuclear reactors and especially designed or prepared equipment and components for nuclear reactors.

The Atomic Energy Act of 1954, as amended: Provides DOE unique authority to perform a broad range of activities related to nuclear weapons. DOE has now invoked Sections 91.c (restricts the release of non-nuclear parts of atomic weapons or the utilization of facilities whose disclosure would contribute significantly to another nation's atomic weapon capability) and 148 (prohibition against the dissemination of certain unclassified information).

International Traffic in Arms Regulations, DOS (22 CFR 120-130): All items Military; contains the U.S. Munitions List

Export Administration Regulation: U. S. Department of Commerce Dual Use Items – Controls all items and technology over which no other agency has jurisdiction. Controls are based on technology, end-user, location, and use.