Subcontract contains **UCNI** ☐ **CUI** ☐ **Both** ☐ **Unclassified Only** ☐

Protection of UNCI / CUI

SELLER shall be responsible for protecting all Unclassified Controlled Nuclear Information (UCNI) and Controlled Unclassified Information (CUI), and materials in connection with the performance of the work under this Purchase Order and in accordance with the CNS UCNI/CUI Protection Program requirements in accordance with the U.S. Department of Energy/National Nuclear Security Administration (DOE/NNSA) Classification Program, DOE CUI Program, NNSA Enterprise Cybersecurity Program Plan (ECSPP), CNS ECSPP Addendum and the CNS UCNI/CUI Protection Program outlined in Appendix A. SELLER shall protect against sabotage, espionage, loss, and theft of UCNI/CUI and/or otherwise controlled materials in SELLER's possession.

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. (i.e., computer, network, system).
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. Includes security protocol standards.
AIS storage media	A means used by AIS systems to convey or store information.
Controlled Unclassified Information (CUI)	Unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy. Includes two (2) categories (or types): Basic and Specified.
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 (IOSC)	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, CUI, 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) ***[LEGACY INFORMATION]***	As of February 2022, now identified as 'Legacy' information. OUO information is unclassified sensitive information which may be exempt from public release under the Freedom of Information Act (FOIA). DOE 'Waiver of CUI Marking Requirements for Legacy Information and Data' applies to handling and protection of this class of information.
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 require specific controls, 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)	Unclassified but sensitive information concerning nuclear material, weapons, design of production facilities, utilization of weapons or components, security measures for the protection of facilities, materials, and information. This information is prohibited from unauthorized dissemination under Section 148 of the Atomic Energy Act, revised. Reference 10 CFR 1017 & Atomic Energy Act of 1954, revised.

SELLER Responsibilities

REQUIRED SELLER UCNI / CUI TRAINING

All vendor personnel handling UCNI/CUI must complete the required **on-line briefing** and **acknowledgement agreement** for protection of UCNI/CUI provided by the UCNI/CUI Protection team at the following website:
https://www.y12.doe.gov/suppliers/suppliersubcontractor-ucnicui-training

Note: Vendor is required to accomplish briefing and acknowledgement every two (2) years

SELLER:

- Must complete the UCNI/OUO/CUI Protection briefing before access to UCNI or CUI is authorized
- Is responsible for safeguarding, handling, possessing, or processing UCNI, OUO, or CUI and shall be responsible for control of any UCNI/OUO/CUI documents, media, other controlled materials, and is not relieved of this obligation for documents provided to others
- Shall ensure that all SELLER personnel and Lower-tier subcontractors and/or suppliers who require access to UCNI or CUI relating to the contract complete the same requisite briefing prior to being provided access to UCNI/CUI
- Will provide the BUYER with briefing records of all individuals briefed including lower-tier subcontractors and/or suppliers upon request
- Maintains current UCNI/CUI Protection briefing records for all SELLER personnel responsible for safeguarding, handling, possessing, or processing UCNI/CUI
    - Note: Additional briefings or instructions may be directed by the BUYER at the BUYER's discretion

GENERAL REQUIREMENTS AND GUIDANCE

SELLER will:

- Ensure UCNI/CUI is:
    - Granted only to U.S. Citizens with a valid need-to-know and is not released without review for release guidance and/or dissemination restrictions
    - Not released to foreign nationals unless otherwise authorized or directed by CNS
    - Not placed on the SELLER's computing equipment/Automated Information System without prior approval of the SELLER's Information System Security Plan (ISSP) by CNS Cybersecurity or otherwise authorized by guidance contained within this form

- Ensure all hard copy UCNI/CUI is returned to the BUYER or STR when no longer contractually required, or properly destroyed with a statement of destruction provided to the BUYER or STR (SELLER must coordinate with STR prior to any attempted destruction)
- Ensure return of all UCNI / CUI 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
- Lower-tier subcontractors and/or suppliers are approved by the BUYER prior to providing electronic or hard copy UCNI/CUI; Flow these requirements down to all lower-tier subcontractors and/or suppliers
- Immediately notify the Y-12 Operations Center (OC) [formerly known as the Plant Shift Superintendent] at 865-574-7172 of any known or suspected security breaches. Cooperate with Network Operations Center/Security Operations Center (NOC/SOC) requirements as directed
- Be responsible for:
    - Recognizing the sensitivity of information before it is stored, processed, or transmitted on any information system; UCNI / CUI can only be stored, processed or transmitted on a system approved by CNS Cybersecurity
    - Safeguarding, handling, possessing, and/or processing UCNI or CUI in accordance with DOE and CNS UCNI/CUI Protection Program requirements

SELLER Access to UCNI / CUI

Access to UCNI shall be provided only to those authorized for routine access in accordance with 10 CFR 1017. Routine access refers to the normal exchange of UCNI during the conduct of official DOE/NNSA business. An authorized individual, who may be the originator or possessor of UCNI, may grant routine access to UCNI to another person, who is eligible for routine access to the information based on 10 CFR 1017. Specific criteria for U.S. citizens vs. non-U.S. citizens must be observed.

The following assurances and requirements below must be met:

- Individual has completed the required CNS UCNI / CUI on-line briefing ("**Identification and Protection of UCNI/OUO/CUI at Facilities External to CNS**")
- Determine Citizenship:
    - U.S. Citizenship. SELLER retains copies. Determination may be obtained 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 (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)

- If non-U.S. citizen requires access, then contact the STR or CNS UCNI Program Manager for additional guidance

- Access limited to need-to-know. A person must possess a valid "need to know" for the specific UCNI or have a government purpose to access UCNI or CUI in the performance of official duties

SELLER UCNI/CUI Work Area and/or Vendor Computer Equipment Approval

UCNI/CUI must be controlled at all times to prevent unauthorized access. If SELLER must establish an **UCNI processing area** at the SELLER's location, then notification must be submitted by the SELLER to the BUYER. The CNS UCNI Program Manager may coordinate with the SELLER to assess/audit the SELLERS intended or established UCNI processing area.

If government-furnished equipment (GFE) is required in order to process UCNI or another class of sensitive government information, then coordination with the BUYER to obtain GFE must be accomplished. Contact CNS Procurement.

If the SELLER desires to use their **Automated Information Systems** (AIS) / computing system to process UCNI electronically, then the SELLER must contact the BUYER (CNS UCNI Program Manager and Cybersecurity Representative(s)) to coordinate approval of the vendor AIS.

- Approval of vendor AIS must be documented via an Information Systems Security Plan (ISSP) 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 Program Manager, CNS Cybersecurity and NIST SP 800-171. An ISSP shall be prepared and approved by CNS Cybersecurity for each system that processes UCNI, and/or other types of sensitive CUI if required by law. **Contact the CNS UCNI Program Manager or Cybersecurity for guidance**

When the SELLER requests an UCNI processing area for approval and/or AIS approval, the BUYER will contact the SELLER to ensure appropriate protection measures are in place and will schedule an inspection at least 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 and/or an AIS assessment prior to need.**

Approval by CNS Cybersecurity is required prior to electronic processing of UCNI 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 Program Manager, CNS Cybersecurity and/or Y-12 Field Office (YFO) will/may perform regular and unannounced surveillances relative to approved information, computer, and physical protection plans.

Approval is required by the CNS UCNI Program Manager and CNS Cybersecurity prior to commencing construction, modification, or declaration of an UCNI processing area or computer equipment.

SELLER Physical Security Requirements

UCNI/CUI documents/materials shall be kept secure at all times in accordance with 10 CFR 1017 or other applicable laws, regulations, government-wide policy (LRGWP), to effectively safeguard information and 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. SELLER must ensure the following physical security measures are met:

- Areas or rooms in which UCNI is stored or processed, must have access controls implemented to limit access and ensure only authorized individuals have access to UCNI materials
    - When UCNI is "In-Use": Areas that process document/materials marked as UCNI must be capable of preventing unauthorized access to such information while 'In- Use'
    - UCNI "Storage": Areas must be capable of properly securing documents/materials marked as UCNI when UCNI is no longer 'In-Use.' Authorized Individuals must be able to effectively secure UCNI in locked receptacles as defined in 10 CFR 1017 (e.g., file cabinet, desk drawer, safes, etc.) if UCNI area resides in an unsecured area or facility
- Access controls/systems must be controlled by the information security point of contact to ensure only individuals with appropriate access may obtain access to UCNI or UCNI areas
- Government-furnished equipment (GFE) computing systems (i.e., laptop, etc.) obtained through CNS channels for execution of the contract are to be regarded as UCNI materials/devices, as they are capable of processing information up to and including UCNI data
    - GFE utilized at the vendor site must secure the devices in approved lockable UCNI processing areas or rooms, or secure when not in use, in accordance with storage requirements as defined in 10 CFR 1017
- Telephones (landline, VOIP) are allowed within the room, HOWEVER:
    - UCNI discussion over unsecure communications is prohibited. UCNI discussions require a secure phone capability (e.g., Secure Telephone Equipment, vIPer)

- Physical processing/work areas may be used for other tasks associated with subcontractor activities when all UCNI/CUI matter is secured/locked in separate lockable containers. If the perimeter of the area is access controlled due to the entire area being a UCNI area, then 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 UCNI or CUI processing area
- SELLER Personal / Company Workstations

Ensure physical access control for the information and employ access restrictions. Access to the computer and associated data may be 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/CUI information shall be positioned to prevent viewing by unauthorized personnel

SELLER Automated Information System (AIS) Requirements

UCNI/CUI, deliverables or working materials provided by the BUYER or SELLER in support of the Purchase Order shall be performed on BUYER approved AIS resources unless otherwise directed or authorized, and shall operate in compliance with any required CNS Cybersecurity approved AIS Security Plan.

SELLER must meet the specific CNS directed Cybersecurity requirements, and directives as defined in Appendix A, as applicable.

SELLER shall submit a request to the BUYER for approval inspection by CNS Cybersecurity.

- <u>Computer Media and Encryption Requirements</u>
    - Computer media containing UCNI/CUI 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/CUI. UCNI/CUI requires removable media including boot drives and drives in which data is contained. In cases where UCNI/CUI 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

- System hardware components shall be marked to indicate the most restrictive category of information processed, as directed by the BUYER
- All media must be encrypted by BUYER approved FIPS 140.2 Level 1 or higher encryption methods
- If required, the SELLER shall install encryption software in compliance with BUYER instructions

An AIS processing UCNI or certain sensitive CUI shall be re-approved by the BUYER every three (3) years or unless otherwise directed by CNS Cybersecurity, 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. Any new computing systems or networks shall be documented and approved by the BUYER (CNS Cybersecurity) prior to use and connection to CNS networks or domains.

- 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 or approved to process the information
- Protect UCNI/CUI to which these owners have access or custody in accordance with security requirements identified in this document

SELLER UCNI/CUI Protection Security Point(s) of Contact

Security Point-of-Contact. 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/CUI protection. The responsibilities of the position include but are not necessarily limited to:

- Represent the SELLER/lower-tier subcontractors and/or suppliers concerning UCNI/CUI Protection issues
- Ensure implementation of, and compliance with, all UCNI/CUI protection requirements
- Report security-related incidents to the BUYER and participating in the inquiry of security incidents. SELLER may contact the following centers 24/7:
  - Y-12 Operations Center - 865-574-7172
- Determine UCNI/CUI Protection briefing/training needs and ensuring briefing/training is conducted in a timely manner
- In coordination with the BUYER or STR, disseminate periodic UCNI/CUI protection awareness material to employees who have responsibilities that include protection and control of controlled information
- Attend 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:

- Ensure the implementation of, and compliance, with the AIS Security Plan
- Represent the SELLER/lower-tier subcontractor and/or supplier for computer security issues
- Coordinate general AIS security briefings/trainings
- Report Computer/AIS-related security incidents to the BUYER and participating in the inquiry of cyber security incidents.
    - Y-12 Operations Center - 865-574-7172
- Coordinate approval of computer systems processing UCNI/CUI with the BUYER (CNS Cybersecurity)
- Ensure AIS system described by the AIS Security Plan has been approved prior to use
- Immediately act to resolve AIS security deficiencies

SELLER Document Requirements

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.

- Reproduction. Reproduction of UCNI/CUI shall not be performed by the SELLER without prior approval of reproduction equipment by the BUYER
- Document Classification. No BUYER or SELLER information associated with CNS is released without review and approval by BUYER. Contact the CNS Classification Office for release restrictions. Only the BUYER or a BUYER-trained and certified individual will classify and mark documents. SELLER shall protect any documents contained in the Purchase Order at the highest level marked. 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

SELLER Transmission of UCNI/OUO Information

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

- Electronic Transmission of UCNI/CUI
    - No transmissions via computer of UCNI will be allowed unless formally pre- approved by the BUYER (i.e., vendor certified systems or GFE)
    - Electronic media transmissions shall be encrypted using BUYER approved FIPS 140- 2 Level 1 or higher encryption modules, or as directed by the BUYER UCNI/CUI Protection team and/or Cybersecurity POC

- Email of UCNI requires encryption and may only be disseminated to/from approved recipients and systems (i.e., AIS) certified to process this class of sensitive government information
- Email of CUI requires encryption. However, if encryption is not available, then password protection is directed

- Telephone Transmissions
  - All voice transmissions of UCNI 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/CUI Protection team and Cybersecurity Lead
  - Although encryption is not required for phone transmissions of CUI, persons should consider if the sensitivity level of the CUI merits encryption when discussed over phone lines
    - CUI specified may have additional encryption requirements based on LRGWP
    - Contact the CNS Classification Officer and/or UCNI/CUI protection team for information related to voice transmission of UCNI/CUI over government- furnished equipment
- Fax Transmission
  - UCNI transmissions are prohibited
  - CUI transmissions 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 the recipient 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 meets any requirements as directed by LRGWP. 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
  - A single opaque envelope, wrapper or coversheet may be used
  - Internal mail systems must use a sealed opaque envelope marked TO BE OPENED BY ADDRESSEE ONLY
  - Authorized individuals may hand carry matter as long as they can control access
- Document Transmission Outside an Approved Facility
  - Documents marked as UCNI or CUI shall be packaged in a single, opaque envelope or wrapping. The envelope shall be sealed and marked 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 using a signature service may be used
- Authorized individuals may hand carry matter as long as they can control access

SELLER Destruction of UNCI / CUI

- UCNI/CUI documents generated as part of daily work that requires disposal may be destroyed using an approved cross-cut shredder. Shred is required to be no greater in size than 1mm x 5mm
- If the SELLER is unable to meet this shred requirement, then alternate destruction methods must be accomplished with the BUYER. Documents that cannot be destroyed using approved shredders (e.g., media, mylar, etc.) must be returned to the BUYER

SELLER Return of UCNI / CUI for Destruction

A SELLER awarded a contract shall return UCNI/CUI electronic data and all media used to process UCNI/CUI supplied by the BUYER or generated by the SELLER, or lower-tier subcontractors, at the termination of the Purchase Order or upon termination of the certification of the computer.

- When lower-tier subcontractors and suppliers have completed their work, the associated data media and materials shall be forwarded to the SELLER
- At the termination of the Purchase Order, the SELLER shall provide written notification to the BUYER stating all UCNI/cui was destroyed or returned to the BUYER
- BUYER will sanitize AIS equipment to remove all UCNI/CUI at the end/termination of contract
- SELLER and BUYER will retain an accountability of media and contents

SELLER Infractions and Incidents

Failure to comply with BUYER directed UCNI/CUI requirements may result in an Incident of Security Concern (IOSC).

- SELLER is responsible for SELLER costs incurred because of IOSCs due to SELLER error

  NOTE: Any person who violates applicable civil law under the 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. Contact Y-12 Operations Center at 865-574-7172. The SELLER shall cooperate with the Network Operations Center/Security Operations Center (NOC/SOC) at 806-477-6010, and with the Y-12 Incident of Security Concerns (IOSC) organization in the conduct of an inquiry of an incident

- All computer security incidents involving UCNI/CUI or AIS resources shall be reported immediately to the BUYER (or Y-12 Operations Center), including:
  - Fraudulent action involving AIS
  - Processing of information without an approved Security Plan
  - Leaving a session active while not properly protected (e.g., unattended, unsupervised)
  - Unauthorized testing of an approved AIS
  - Printer ribbons, cards, diskettes, hardcopy output, and/or magnetic media left unattended (not properly physically protected)
  - Disclosure of sensitive information (e.g., failure to protect data files properly)
  - Hackers/crackers or other unauthorized access attempts
  - Using CNS UCNI on unapproved/uncertified AIS
  - 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 471.7, Controlled Unclassified Information
4. DOE Policy 7 (POL-7) “Implementing Controlled Unclassified Information (CUI) for Department of Energy (DOE) Classification Guides and Bulletins”
5. DOE Policy 8 (POL-8) “Clarification of Unclassified Controlled Nuclear Information Requirements under Controlled Unclassified Information”
6. DOE O 205.1C, 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 Non-federal Systems and Organizations

Applicable CNS Procedures and Policies

1. Y19-401, Automated Information System (AIS) Security Handbook
2. Y15-404, Acceptable Use of Information Technology
3. CNS E-PROC 0043, CNS Export Compliance Procedure
4. CNS E-PROC 3123, Identification and Protection of Unclassified Controlled Nuclear Information and Controlled Unclassified Information
5. NNSA Enterprise Cybersecurity Program Plan
6. CNS Addendum to the NNSA Cybersecurity Program Plan

Appendix A

1. Purpose

This Appendix defines the requirements for the Identification and Protection of Unclassified Controlled Nuclear Information (UCNI), [LEGACY] Official Use Only (OUO) Information, and Controlled Unclassified Information (CUI). It further outlines responsibilities of the SELLER to comply with the Contractor Requirements Document (CRD) of referenced orders and flowing down the CRD requirements to the subcontractor(s) at all tiers, to the extent necessary to assure contractor compliance.

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.

3. Other Documents Needed

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

4. References

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

5. Roles and Responsibilities

5.1 CNS Classification Officer

1. Appointed and designated to administer the UCNI Protection Program at the Y-12 National Security Complex (NSC).
   a. Serves as lead UCNI Reviewing Official (RO) for both sites.
   b. May delegate personnel to execute various aspects of UCNI administration in support of DOE O CRD information protection program action requirements.
2. Every two (2) years at minimum, IAW DOE O 471.1B Contractor Requirements Document (CRD), prepares written self-assessment of the implementation of the UCNI program requirements, including corrective action plans for any deficiencies noted.
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.

Appendix A (Cont.)

5. Utilizes current UCNI guidance to develop detailed contract-level UCNI guidance, tailored to the needs of 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.
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. Guides development, approval and interpretation of policies and procedures for Y-12 UCNI protection in accordance with applicable DOE/NNSA directives.
11. Serves as the liaison between Contractor and the Y-12 Field Office (YFO) for UCNI protection matters.

5.2 CNS Subcontract Procurement Representatives (BUYER)

1. Coordinates with the Subcontract Technical Representative (STR) and Subcontractor Company whenever procurement activities may involve UCNI/CUI protection.
2. Employs UCN-26608, UCNI/CUI Protection Requirements for CNS Suppliers to ensure identification and protection requirements for UCNI/CUI are addressed in procurement contracts.
3. Acts as a liaison between the Subcontractor Company and CNS on all UCNI/CUI protection matters, as defined by the subcontract and UCN-26608.
    a. Notifies the Subcontractor Company: IF subcontractor will be handling and generating UCNI/CUI, THEN subcontractor is directed to obtain UCNI/CUI protection awareness training (online course) and encouraged to coordinate with the CNS Classification Office to have personnel handling UCNI, be certified as DOE UCNI Reviewing Officials (RO).
4. Employs UCN-22435 to identify citizenship of the vendor/subcontract company representative, and determine a need-to-know prior to granting access to UCNI.
5. Notifies the CNS UCNI/CUI Protection and CNS Cybersecurity Teams when an off- site facility is going to be generating UCNI/CUI.

Appendix A (Cont.)

5.3 Subcontract Technical Representative (STR) Assigned to Subcontractor Company

1. Acts as a liaison between the Subcontractor Company and CNS on all UCNI/CUI protection matters as defined by the subcontract.

2. Employs UCN-26608 to ensure subcontractors and potential contractors that access, use, or generate UCNI/CUI:
   a. Receives and understands the appropriate training prior to having access to UCNI/CUI in accordance with UCN-26608.
   b. Understands the requirements for protecting, marking, and transmitting UCNI/CUI.
   c. Complies with the contract-based classification, Identification and Protections requirements.
3. Ensures that the appropriate language for protecting UCNI/CUI is a part of a Subcontractor Company's Statement of Work (SOW) and eventual subcontract.
4. Brings any concerns of potential UCNI/CUI mishandling to the immediate attention of the Procurement Representative and the Classification Office.
5. Ensures all UCNI/CUI is retrieved from the subcontract company when no longer contractually required, or a statement of destruction is obtained.

5.4 Subcontract Companies

1. Employs UCN-26608 to:
   a. Identify/appoint an UCNI/CUI Protection Point of Contact (POC) and Computer Security POC to coordinate and interface with the CNS UCNI/CUI Protection and CNS Cybersecurity Teams, and ensure the necessary physical security and cybersecurity measures are in place in order to properly protect UCNI/CUI.
   b. Ensure UCNI/CUI contract provisions, laws, regulations are effectively accomplished.
   c. Provide oversight of all subcontractor employees and ensure compliance with UCNI/CUI Protection Program requirements.
   d. Determine appropriate need-to-know for all subcontract employees in accordance with specific UCNI requirements.
2. Maintains all records regarding the protection of UCNI/CUI 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.

Appendix A (Cont.)

4. Ensures all UCNI/OUO information/CUI 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 must know the identity of and how to contact the UCNI RO, in order to coordinate reviews of documents generated by the company.

   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.

5.5 Authorized Holder (AH)

1. An individual, organization, or group of users that is permitted to designate or handle CUI, consistent with the guidelines in DOE O 471.7, 32 CFR 2002, and the CUI Registry.

6. Unclassified Controlled Nuclear Information

6.1 What is 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 What is the UCNI Review Process

1. Reviewing documents for UCNI - Anyone who originates or possesses a document that they believe 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. The term 'Organization' is defined as the company (i.e., vendor, subcontractor) and the project staff (i.e., Y-12, 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.

Appendix A (Cont.)

4. Upon review and 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.

5. 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.

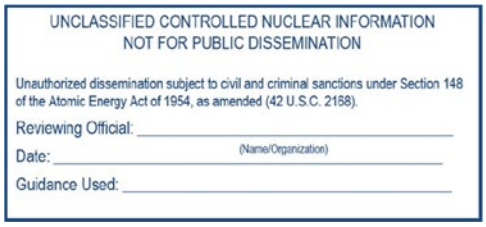
6.4 UCNI Markings on Documents or Material

Note: IMPORTANT: DO NOT USE National Archives and Records Administration (NARA) directed UCNI markings. DO NOT USE: "CUI//SP-UCNI" marking. DOE Office of Classification has directed that UCNI markings remain consistent with UCNI Law 10 CFR 1017. See DOE Policy 8 for more information.

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: _____

Appendix A (Cont.)

2. Marking Pages: The marking ‘‘Unclassified Controlled Nuclear Information’’ must be placed centered on the bottom of the front of the document and on the bottom center 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/reveals UCNI regardless of any other unclassified control marking (e.g., CUI) that is also contained in/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.

   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.

4. 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 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.

Appendix A (Cont.)

5. 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.

   a. Any electronic transmission of UCNI requires encryption technology that adheres to requirements set forth in 10 CFR 1017.

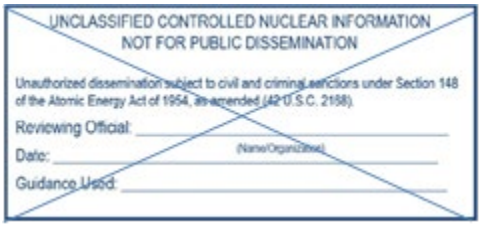
6. Transmittal Documents: A document that transmits documents or material marked as containing UCNI and does not itself contain classified information or UCNI must be marked on the front of the document as indicated below. If the transmittal document does not itself contain UCNI, no UCNI markings should 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

Only the Reviewing Official (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 RO may line through the "UCNI" marking and 'X' through the previous UCNI signature block. The official marks or authorizes the marking of the document (or the material, if space allows) as follows:

~~UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION~~



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

Appendix A (Cont.)

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. On-line vendor training provided by the BUYER supports this notification process.

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 UCNI - 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. Eligibility is as follows:

      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

Appendix A (Cont.)

A person who is not a U.S. citizen but is: **1)** A Federal Government employee or a member of the U.S. Armed Forces; **2)** An employee of a Federal Government contractor or subcontractor; **3)** A Federal Government consultant; **4)** A member of a DOE advisory committee; **5)** 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; **6)** An employee or representative of a State, local, or Indian tribal government; or, **7)** 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 10 CFR 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.

Appendix A (Cont.)

5. Destruction: Although 10 CFR 1017 allows destruction of UCNI via a cross-cut shredder that produces particles no larger than ¼" X 2", DOE O 471.7 requires shred to be no greater than 1mm X 5mm. It is recommended that the SELLER employ the smaller shred of UCNI. The SELLER may coordinate with the STR to request alternative destruction methods that may be available (i.e., Destruction and Recycling (DAR) bins).

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 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, or is certified for classified information.

Appendix A (Cont.)

Note 1: ATTENTION: UCNI email sent between government and vendor systems is prohibited unless CNS Cybersecurity has certified and authorized vendor AIS to process this class of sensitive government information.

Note 2: All UCNI E-mail messages sent between **y12nsc.doe.gov,** and **yfo.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 addresses.

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.

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. Controlled Unclassified Information (CUI)

7.1 Identifying and Marking CUI

To be identified as CUI, information must be information the government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, and that LRGWP requires or permits an agency to handle using safeguarding or dissemination controls

1. **Identification.** Federal unclassified information created or originated by the contractor, produced by or for the contractor, or under the control of the contractor, through a DOE contractual mechanism, that has been determined to be CUI (per Departmental Element direction, LRGWP), is identified as containing CUI.

Appendix A (Cont.)

2. **Marking.** Documents and matter determined to contain CUI are marked appropriately as defined in the DOE approved CUI list. Except for Unclassified Controlled Nuclear Information (UCNI), and Critical Energy Infrastructure Information (CEII), and Naval Nuclear Propulsion Information (NNPI), CUI markings are the only markings to be used to designate unclassified documents and matter containing CUI.
3. Although the National Archives and Records Administration (NARA) has approved approximately 125 CUI categories for use government-wide, DOE is the final approving authority on which CUI categories will be recognized for use throughout the DOE Complex and its associated sites and M&O contracts.
    a. Contact the CNS Classification Office for more information on the DOE approved CUI list to identify which CUI Categories are currently approved for use in the DOE.
4. For information to be identified as CUI, it must be designated by an Authorized Holder as either of the two (2) types of CUI: CUI (basic) or CUI (specified).
    a. **CUI Basic** is the subset of CUI for which the authorizing LRGWP does not set out specific safeguarding or dissemination controls. CUI Basic is handled according to the uniform set of controls in 32 CFR part 2002, DOE Order 471.7 CUI, and the CUI Registry. If safeguarding and dissemination controls are not contained in the LRGWP, CUI Basic controls apply.
    b. **CUI Specified** is the subset of CUI in which the authorizing LRGWP contains specific handling controls that it requires or permits agencies to use, and which differ from those controls for CUI Basic. Safeguarding and dissemination controls contained in LRGWP take precedence over the requirements in 32 CFR part 2002. CUI Basic controls apply whenever CUI Specified controls do not cover the involved CUI.
5. CUI Basic and Specified. This section identifies CUI basic and specified commonly used within DOE. Additional categories are identified in the DOE approved CUI list.
    a. Privacy Information. Requirements for the marking and safeguarding of personally identifiable information (PII) under CUI are outlined in DOE O 206.1, *Department of Energy Privacy Program*. PII must be handled in accordance to the level of sensitivity, with more sensitive categories, i.e., Social Security Numbers, financial records, and medical records, being safeguarded through encryption or password protection. Privacy information, in either physical or electronic format, which is collected, used, processed, maintained, stored, shared, or transferred within DOE should be marked and safeguarded under the requirements of DOE O 471.7 and 32 CFR 2002. CUI specified markings may be applicable under the Privacy Act of 1974 (Title 5 U.S.C. 522a)
        i. For additional guidance on Privacy and related regulatory requirements, contact the BUYER (CNS Privacy Officer).

Appendix A (Cont.)

b. Export Controlled Information. Information (which may include technology, technical data, assistance, or software), the export (including transfer to foreign nationals within the U.S.) of which is controlled under the "Export Administration Regulations", the "International Traffic in Arms Regulations", "10 CFR 810, Assistance to Foreign Atomic Energy Activities" regulations, or various trade and economic sanctions. Export Control CUI markings may only be placed on documents/materials by an authorized Export Control subject matter expert.

7.2 Identifying and Marking a Previously Marked OUO Document as CUI

1. Previously marked documents bearing Official Use Only (OUO) markings are now considered 'Legacy' documents.

   Per DOE 471.7, documents and matter generated prior to issuance of the Directive or that are maintained in files to which access is restricted are not required to be reviewed and brought to current standards unless they (or a copy of such document and matter) is/are removed from restricted access files and not to be returned; or are distributed outside of DOE; or if a new document and matter is created using information from a 'legacy' document and matter that qualifies as CUI. If any of these conditions are met, then legacy markings must be removed or redacted, the document and matter reviewed, and then re-marked as CUI (if applicable), even if the information was under a legacy material marking equivalency and exemption prior to re-use.

2. Vendors who currently hold previously marked OUO documents may:

   a. Return previously marked OUO materials to CNS for destruction or destroy the OUO materials in accordance with the destruction requirements directed in this document, if the materials are no longer required.

   b. Maintain OUO materials in files and maintain access restrictions until such time that return of materials to CNS is required per contract requirements.

   c. Redact previous OUO markings and remark OUO materials that qualify to be re-marked as CUI, if material is required for use or processing.

   d. Per DOE Policy 7: Previously marked OUO Exemption 7, Law Enforcement, and OUO Exemption 4, Commercial/Proprietary, is to be remarked "CUI".

   e. Coordinate with their respective Subcontract Technical Representative (STR) to ensure appropriate disposition of legacy materials.

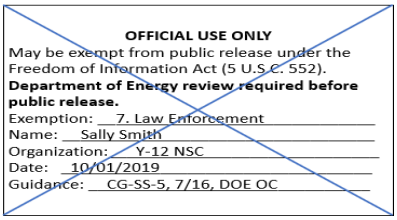
7.3 Removal/Redaction of OUO Markings

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

Appendix A (Cont.)

1. An Authorized Holder with cognizance over the information in a document or material marked as containing OUO may determine that the document or material no longer contains OUO. Individuals making this determination must base it on applicable guidance and ensure that any OUO markings are either crossed out (for documents) or removed (for material). Line through the "OUO" marking and 'X' through the previous OUO signature block. The official marks or authorizes the marking of the document (or the material, if space allows) as follows:

~~OFFICIAL USE ONLY~~



7.4 Relationship of OUO Markings to Other Types of Control Markings

1. Classified Documents: Contact the CNS Classification Office with questions about remarking classified documents that contain OUO markings.
2. Marking Documents Generated Before April 9, 2003: Contact the CNS Classification Office. 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.
3. 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.
4. 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 applicable LRGWP.

Appendix A (Cont.)

7.5 Safeguarding and Physical Protection of CUI

1. Ensure that if an unmarked document and matter is believed to contain CUI, the unmarked document and matter is protected as CUI until it can be reviewed to determine if it contains CUI.
2. CUI that is reproduced (e.g., copied, scanned, printed, electronically duplicated) or shared must be protected the same as the original CUI document and matter in furtherance of a lawful government purpose.
3. Protect CUI from unauthorized access or disclosure and make use of controlled environments. A controlled environment is any area or space an Authorized Holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.
    a. When outside a controlled environment, ensure CUI is protected under Authorized Holder's direct control, or with at least one (1) physical barrier to protect the CUI from unauthorized access or observation. To the extent necessary, ensure that unauthorized individuals cannot inadvertently overhear conversations discussing CUI.
4. Protection in Use: Reasonable precautions must be taken to prevent access to documents marked as containing Legacy OUO and CUI by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don't read a CUI document in a public place, such as a cafeteria, on public transportation).
5. Protection in Storage: Documents marked as containing Legacy OUO or CUI may at minimum 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., safe, a locked file cabinet, desk, bookcase, or briefcase).
6. Reproduction: CUI that is reproduced (e.g., copied, scanned, printed, electronically duplicated) or shared must be protected the same as the original CUI document and matter in furtherance of a lawful government purpose. When reproducing CUI on equipment such as printers, copiers, scanners, or fax machines, ensure to the extent possible that equipment does not retain the unencrypted copied data or CUI related data, and that equipment is sanitized.
7. Destruction: A shredder must be a cross-cut shredder that produces particles no larger than 1mm x 5mm, and it must be checked after every use for compliance.
8. 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."

Appendix A (Cont.)

- 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 CUI 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 CUI 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. Contact the BUYER CNS UCNI Program Manager for additional guidance as necessary.

e. By Unencrypted Facsimile: An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that the recipient can control the document when it is received.

f. By E-mail without Encryption: If encryption is not available, then password protection is directed. The sender can call the recipient with the password so they may access the file.

g. Transmission over Voice Circuits: CUI 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 may be used. Authorized Holders of CUI should consider if the sensitivity of the CUI merits encryption when discussed over the phone or other voice circuit. Contact the BUYER CNS UCNI Program Manager for additional guidance as necessary.

8. Privacy-Related Information

For all Privacy-related information questions, refer to the BUYER (CNS Privacy officer) for additional guidance on handling, safeguarding, storage, processing, and transmission.

8.1 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) immediately upon discovery (i.e., within 10 minutes of discovering the incident).

Appendix A (Cont.)

8.2 Violations

DOE and contractor employees who handle records must ensure administrative, technical, and physical safeguards are in place to protect information from unauthorized disclosure or access by unauthorized persons. Penalties per incident are or may be imposed on individuals who violate certain sections of 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 - (ECI)

Note: **ONLY AUTHORIZED EXPORT CONTROL SUBJECT MATTER EXPERTS MAY IDENTIFY AND MARK CUI WITH EXPORT CONTROL MARKINGS**. Contact the CNS Export Compliance office for more information on ECI.

An Export Controlled document may contain:

1. Unclassified information that reveals technological information that would aide in the development, production, or use of a technology or commodity; that has not been released readily in public domain; 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 CUI//EXPT or CUI//SP-EXPT, CUI// EXPTR, and/or otherwise marked in accordance with export law.

Foreign nationals are not allowed access to ECI unless specifically authorized by the CNS Export Compliance Office. The CNS Export Compliance Office has final determination authority on export controlled information.

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

Appendix A (Cont.)

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 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.