UCNI / CUI Protection Requirements for Pantex Supplier

Subcontract contains UCNI ☐ CUI ☐ Both ☐ Unclassified Only ☐

Protection of UCNI/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 Pantex 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), Pantex ECSPP Addendum. 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. (e.g., 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 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).

Federal Information Processing Standards (FIPS)	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://pantex.energy.gov/about/visiting-us/visitor-training

Note: Vendor is required to complete briefing and acknowledgement every 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 Pantex
    - Not placed on the Seller's computing equipment/Automated Information System without prior approval of the Seller's Information System Security Plan (ISSP) by Pantex Cybersecurity or otherwise authorized by guidance contained within this form
- Ensure all hard copy UCNI/CUI is returned to the Buyer or Subcontract Technical Representative (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 Pantex 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 Pantex Operations Center at 806-477-5000 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 Pantex Cybersecurity
    - Safeguarding, handling, possessing, and/or processing UCNI or CUI in accordance with DOE and Pantex 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 Pantex UCNI/CUI on-line briefing ("**Identification and Protection of UCNI/OUO/CUI for Vendors and Subcontractors**")
- 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 Pantex 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 Pantex UCNI Program Manager or Information Security 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 Pantex 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 (Pantex 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, Pantex Cybersecurity and NIST SP 800-171. An ISSP shall be prepared and approved by Pantex Cybersecurity for each system that processes UCNI, and/or other types of sensitive CUI if required by law. **Contact the Pantex UCNI Program Manager, Information Security 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 Pantex 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 Pantex Cybersecurity prior to implementation.

The UCNI Program Manager, Pantex Cybersecurity, Information Security Manager and/or Pantex Field Office (PFO) will/may perform regular and unannounced surveillances relative to approved information, computer, and physical protection plans.

Approval is required by the Pantex UCNI Program Manager and Pantex 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
- GFE computing systems (i.e., laptop, etc.) obtained through Pantex 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 used 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 Pantex 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 Pantex 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 Pantex 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 Pantex Cybersecurity approved AIS Security Plan.

Seller must meet the specific Pantex directed Cybersecurity requirements, and directives as defined in DOE O 205.1.C.

Seller shall submit a request to the Buyer for approval inspection by Pantex Cybersecurity.

- Computer Media and Encryption Requirements
    - 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 3 years or unless otherwise directed by Pantex 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 (Pantex 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 (Pantex Cybersecurity) prior to use and connection to Pantex 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 (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/CUI protection. The responsibilities of the position include but are not necessarily limited to the following:

- 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 center 24/7:
  - Pantex Operations Center – 806-477-5000
- 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.
    - Pantex Operations Center – 806-477-5000
- Coordinate approval of computer systems processing UCNI/CUI with the Buyer (Pantex 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 Pantex is released without review and approval by Buyer. Contact the Pantex 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 Seller the transmission of UCNI/CUI Information section of this document.

Seller Transmission of UCNI/CUI 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 Pantex Cybersecurity approved encryption methods) and then only after certification by the Pantex 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 Pantex 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 UCNI/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 Pantex Operations Center at 806-477-5000. The Seller shall cooperate with the Network Operations Center/Security Operations Center (NOC/SOC) at 806-477-6010, and with the Pantex 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 the Pantex 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 Pantex UCNI on unapproved/uncertified AIS
  - Connecting certified AIS to an unapproved network

Applicable Regulatory Requirements

- 10 CFR 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*
- 32 CFR Part 2002, *Controlled Unclassified Information*
- DOE O 471.1B, *Identification and Protection Unclassified Controlled Nuclear Information*
- DOE O 471.7, *Controlled Unclassified Information*
- DOE Policy 7 (POL-7) *Implementing Controlled Unclassified Information (CUI) for Department of Energy (DOE) Classification Guides and Bulletins*
- DOE Policy 8 (POL-8) *Clarification of Unclassified Controlled Nuclear Information Requirements under Controlled Unclassified Information*
- DOE O 205.1C, *Department of Energy Cyber Security Program*
- NNSA SD 205.1, *NNSA Baseline Cyber Security Program*
- NIST SP 800-171, *Protecting Controlled Unclassified Information in Non-federal Systems and Organizations*

Applicable Pantex Procedures

- E-PROC-0043, *Export Compliance Procedure*
- MNL-352350, *Identification and Protection of Unclassified Controlled Nuclear Information and Controlled Unclassified Information*