SUBCONTRACTOR CONTROLLED UNCLASSIFIED INFORMATION - INFORMATION PROTECTION & MANAGEMENT OF CUI

What is CUI and why was it established?

Established by Executive Order (EO) 13556 in 2010, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies also known as LRGW. The EO established an open and uniform federal program for managing CUI that protects unclassified information that is considered sensitive. For additional information, please click here.
NOTE: CUI replaces the previous marking requirements for OUO and other legacy markings. However, not all OUO will be CUI.

In February 2022, DOE established the CUI Program and issued DOE O 471.7, Controlled Unclassified Information. The CUI Program standardizes the way DOE handles information that requires protection under LRGWP, but that does not qualify as classified under Executive Order (EO)13526, Classified National Security Information. This Directive implements the requirements in EO 13556, Controlled Unclassified Information, and 32 CFR part 2002, Controlled Unclassified Information.

- **Why protect it?**

  CUI can be the path of least resistance for adversaries. Loss of aggregated CUI is one of the most significant risks to national security. Thus, CUI enables consistent processes to safeguard sensitive information that is not classified.
  - *Everyone is responsible for properly protecting and managing CUI.*
  - *CUI will not be publicly released.*
  - *All CUI emails must be encrypted (or password protected) when transmitting between suppliers or subcontractors & SRNS.*

Types of CUI

There are two (2) types of CUI, Basic and Specified. These levels are determined by the LRGWP that covers each category of CUI.

1. CUI Basic: subset of CUI for which the authorizing LRGWP does not set out specific handling or dissemination controls. CUI Basic is handled according to the uniform set of controls in 32 CFR Part 2002 and the CUI Registry. (i.e. Inventions, Emergency Management, Patent Applications, Physical Security, OPSEC).
2. CUI Specified: subset of CUI where the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing LRGWP does not provide specific guidance. (i.e. General Privacy, Budgeting, Nuclear Security Related Information).

CUI Specified is NOT a "higher level" of CUI, it is simply different.

CUI Registry & DOE CUI Category List

The CUI Registry, found on and maintained by the National Archives and Records Administration (NARA) website, is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. It identifies all approved CUI categories and subcategories government-wide, provides general descriptions for each, identifies the authorities, establishes marking requirements, and includes guidance on handling procedures. Not all CUI Categories on the CUI Registry are authorized for DOE use.

DOE has a specific DOE CUI Category List and must have an authority to use a CUI category. Currently, DOE has 54 identified CUI categories from the CUI Registry that may be used to safeguard and/or limit the dissemination of DOE sensitive information. The DOE CUI Category List provides applicable CUI Basic and/or Specified Banner Marking that may be used to mark material containing CUI.

The CUI Program will narrow down the 54 categories to the most common categories that may be used at the Savannah River Site.

CUI Training & Access

All supplier or subcontractor employees or individuals working on their behalf, who may interact with CUI are required to complete mandatory CUI training TREGSCUI_SP: CUI-100DE, Overview of Controlled Unclassified Information in SITEU (currently available) and must be trained on appropriate handling procedures and requirements once every two (2) years thereafter.

CUI may only be disseminated and shared with persons in accordance with an LGP (lawful government purpose) and those who are eligible for access under applicable LRGWP.

1. No individual may have access to CUI unless they have received the proper mandatory training and determined that they have an authorized LGP.
2. To the extent possible, ensure unauthorized individuals cannot inadvertently observe or overhear conversations discussing CUI.
3. All documents and matter must be reviewed to ensure they do not contain CUI prior to public release. CUI must be removed or decontrolled from documents prior to public release.

CUI Frequently Asked Questions

1. **Can CUI be stored on non-federal information systems e.g., supplier systems?**
    a. Yes. DOE O 471.7 invokes NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, which defines the requirements for protecting CUI information stored on nonfederal information systems. You may access more information about compliance with NIST SP 800-171, here.

2. **How do I protect CUI?**
    a. CUI in physical form, such as paper must be protected in a controlled physical environment (e.g., lockable office, file room, or cabinet, etc.). When safeguarding physical CUI, you must use at least one locked physical barrier to protect CUI from unauthorized disclosure or access of the information. In an electronic environment (e.g., computer, intranet), CUI must be protected in transit and must meet NIST 800.53 Rev 5 moderate level to prevent unauthorized disclosure or access of the information. Most DOE unclassified networks meet this baseline requirement, but, if in doubt, speak to your IT or cyber security POC.

3. **How is CUI protected in an electronic environment (e.g., computer, intranet)?**
    a. CUI must be stored in a system that meets NIST 800.53 Rev 5 Moderate level controls. Access controls should be in place to limit access to individuals who need access for a Lawful Government Purpose (LGP). Procurement Representatives & Suppliers should work with information security to verify their systems may receive CUI.

4. **Is encryption required for CUI transmission via phone?**
    a. No. For phone transmission, encryption is not required.

5. **Is encryption required for sending CUI information via email between SRS & suppliers or subcontractors?**
    a. Emails that contain CUI information must be protected in transit. When sending CUI via email to accounts outside of site network boundary, the CUI must be in an attachment and protected by encryption or password protection. If a password is used, the password must be transmitted separately from the email attachment containing CUI (e.g., by phone, text, encrypted email).

6. **What is the guidance on whether non-U.S. citizens can receive/view OUO/FOUO information?**
    a. Access to CUI should be encouraged and permitted to the extent that access or dissemination abides by the laws, regulations, or Government-wide policies that established the information as CUI and furthers an LGP.
    Reference the CUI Registry: Limited Dissemination Controls for guidance on CUI dissemination.

7. **What is the CUI Registry and where can I find it?**
    a. The CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
    The CUI Registry can be found at: www.archives.gov/cui. Please note, not all categories identified on registry are eligible for use by SRS.

8. **How will the CUI program change the way sensitive unclassified materials are handled at DOE?**
    a. DOE changes include, but are not limited to:
        - Discontinue the use of OUO and other legacy markings used to label sensitive information;
        - Update legacy markings to the applicable CUI label when creating new, reusing old documents, and/or sharing information outside of DOE;
        - Contract updates including the use and management of CUI;
        - Amend some DOE Directives and regulations;
        - Change electronic forms and update instructions for their submission if they contain legacy markings; or
        - Update data systems that store, mark, identify, and share sensitive information.

9. **How are CUI documents marked?**
    a. SRS employees and subcontractors must receive training prior to marking any documents. Only CUI markings listed in the DOE Category List and on the SRNS CUI SharePoint are authorized for use when designating unclassified information that requires safeguarding or dissemination controls. All CUI must be marked with a CUI Banner Marking. The primary control marking for all CUI at DOE is the "CUI" acronym which must be centered when feasible and appear in CAPITALIZED bold black text at the top of each page of any document that contains CUI. The CUI Banner Marking must be inclusive of all CUI within the document and must be the same on each page. As an optional best practice, the banner marking may also be placed at the bottom of each page of the document.

    Structure the CUI Banner Marking as follows:
        - Separate the CUI control marking with double forward slash (//) before the Category Acronym
        - Include category acronym for all CUI contained in document as follows:
        - Basic – DOE has the option to mark a document that contains CUI basic is "CUI", or the "Alternative Banner Marking for Basic Authorities" published on the CUI Registry for categories DOE has the authority to use.
        - Specified – Category acronym preceded by SP and a dash "SP-"
        - Alphabetize and separate multiple categories with a single forward slash (/) on each page.
          Example of CUI Banner Markings:
          CUI Basic: CUI//INVENT
          CUI Specified: CUI//SP-BUDG

10. **As a supplier, how would I identify CUI in an email?**
    a. When SRS personnel share CUI outside of the SRS network, it must include a CUI banner marking to alert recipients the type of CUI in their possession.
    If CUI is shared electronically through email the following applies:
        - Proper CUI banner marking as the first line in the email in banner format must be included.
        - Attachments containing CUI must be marked appropriately.
        - If the message itself is not CUI but contains an attachment with CUI, the message must indicate that the attachment is CUI and that when separated, the email does not contain CUI

11. **What happens if SRS forgets to mark the document before transmitting CUI?**
    a. If SRS personnel forget to mark documents or emails containing CUI when sharing the information with authorized recipients outside of the SRS network, SRS personnel will contact the recipient to provide notification of omission of CUI marking, advise the recipient that the information contains CUI, and provide an updated, marked version as soon as possible.

12. **How do I dispose of CUI?**
    a. CUI should be destroyed or shredded in a manner that makes it unreadable, indecipherable, and irrecoverable. When CUI Specified information is to be destroyed and the applicable LRGWP specifies destruction requirements, the LRGWP must be followed. A document containing CUI may be destroyed using a cross-cut shredder producing particles no larger than 1 mm x 5 mm (0.04-inch x 0.2-inch) particles. *NOTE: Suppliers may need to return CUI documents to SRS for destruction.*

13. **What is the process for responding to the potential misuse of CUI?**
    a. Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in this procedure, DOE O 471.7, 32 CFR part 2002, the CUI Registry, or the applicable laws, regulations and government-wide policies that govern the affected information. Misuse of CUI, in printed or electronic form, must be reported in accordance with the requirements provided in the SRS M&O CUI procedure to the SRS-M&O CUI Program Manager and Field Element Liaison. Any misuse of CUI Specified may be considered as an Incident of Security Concern (IOSC) under DOE O 470.4, Safeguards and Security Program. The SRS-M&O IOSC program has incorporated the intentional mishandling of CUI into applicable procedures for NNSA-SRFO and DOE-SROO IOSC Program Plans.

       The types of reportable misuse include:

       - CUI from a document and matter marked as containing CUI is intentionally released to a person who does not have a LGP requiring access to the information to perform his or her job or other DOE authorized activities.
       - A document and matter marked as containing CUI is intentionally or negligently released to a person who does not have a LGP requiring access to the information to perform his or her job or other DOE-authorized activities.
       - A document and matter that is known to contain CUI is intentionally not marked.
       - A document and matter that is known to not contain CUI is intentionally marked as containing such information.

Questions? Contact Us:
Savannah River Nuclear Solutions
Ask_SCM@srs.gov