CONTROLLED
UNCLASSIFIED
INFORMATION

TRAINING REFERENCE GUIDE
FOR INDUSTRY

WHEN IS CUI TRAINING REQUIRED?

CUI training is required for Industry when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements. DOD contractors are required to take training annually. This requirement is different than requirements found in the 32 CFR 2002, which requires training every two years. Industry may take training developed and offered by the Center for Development of Security Excellence (CDSE) or it may create its own training program, based on guidelines, supporting law, regulation, or government wide policy protecting CUI. Questions regarding CUI training requirements should also be directed to the responsible GCA.

HOW IS THE CDSE CUI TRAINING ACCESSED?

The CDSE CUI training is located https://www.cdse.edu/Training/eLearning/IF141/.

The training is self-paced and may be accessed at any time. A training certificate is provided when successfully completed.

Industry is also encouraged to supplement CUI training by taking Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI) (IF130.16) at https://www.cdse.edu/Training/eLearning/IF130/. This will help to protect CUI and and may help minimize any serious adverse effects of unauthorized disclosure to the organization, organizational operations, assets, and personnel.

WHAT DOES CUI TRAINING COVER?

CUI training requirements are outlined in the DOD 5200.48 and the ISOO CUI Notice 2016-01: Implementation for CUI Program. Additional information may be found at:

- https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF
- https://www.archives.gov/files/2016-cuio-notice-2016-01-implementation-guidance.pdf

11 REQUIRED CUI TRAINING TOPICS

All CUI training, including any custom Industry training must address the following 11 items:

1. Identify the offices or organizations with oversight responsibility for the CUI Program

Department of Defense DODI 5200.48 identifies departmental officials and elements with oversight responsibilities within DOD.

The CUI Executive Agent (EA) assigned to National Archives and Records Administration (NARA) implements the Order for the CUI program and oversees agency actions to ensure compliance.

The Information Security Oversight Office (ISOO) exercises EA responsibilities for the CUI Program. Title 32 CFR Part 2002, Controlled Unclassified Information (September 14, 2016), establishes CUI Program requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.

The DOD CUI Senior Agency Official - Under Secretary of Defense for Intelligence and Security (USD(I&S)) establishes policy and oversees the DoD Information Security Program.

The DOD CUI Senior Program Manager - Director for Defense Intelligence (Law Enforcement, Counterintelligence, and Security) (DDI(CL&S)) Oversees and manages the DOD CUI Program in coordination with the Secretaries of the Military Departments, Under Secretary of Defense for Research and Engineering (USD(R&E)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the DOD Component heads. Together they provide guidance on DOD Component implementation policy and uniform standards to display CUI controls and banners for DOD systems and networks in coordination with the DOD Chief Information Officer (CIO).

The Director, Defense Counterintelligence and Security Agency has oversight of the CUI Program relating to the National Industrial Security Program (NISP).

2. Convey individual responsibilities related to protecting CUI — 32 CFR 2002.14 (c)

Authorized holders must take reasonable precautions to guard against unauthorized disclosure of CUI. They must (1) establish controlled environments in which to protect CUI from unauthorized access or disclosure; (2) reasonably ensure that CUI in a controlled environment cannot be accessed, observed, or overheard by those who are not authorized; (3) keep CUI under the authorized holder's direct control or protect it with at least one physical barrier; (4) protect the confidentiality of CUI that agencies and authorized holders process, store, or transmit on Federal information systems in accordance with the applicable security requirements and controls established in NIST SP800-53.

3. Describe the differences between CUI Basic and CUI Specified

CUI Basic: The subset of CUI for which the authorizing law, regulation, or government-wide policy DOES NOT set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR 2002 and the DOD CUI Registry.

Example CUI Banner Marking for CUI Basic:
CUI//AAAA//DISSEM

CUI Specified (SP): The subset of CUI for which the authorizing law, regulation, or government-wide policy requires specific protections in handling controls. The underlying authority spells out the controls for CUI Specified (SP) information for safeguarding and does not for CUI Basic information.

Example CUI Banner Marking for CUI Specified or Limited Dissemination Control Marking (must appear at the top of the document):
CUI//SP-SPECIFIED-A/SP-SPECIFIED-B//DISSEM

4. Identify the organizational index with categories or subcategories routinely handled by agency personnel and any special handling requirements (i.e., for CUI Specified)

CUI categories and subcategories are the exclusive designations for identifying unclassified information that a law, regulation, or Government-wide policy requires or permits agencies to handle by means of safeguarding or dissemination controls as stated in 32 CFR 2002.12(a). A CUI category may be listed Specified, while some or all of its subcategories may not be, and vice versa. If dealing with CUI that falls into a CUI Specified category or subcategory, review the controls for that category or subcategory on the CUI Registry.

5. Describe the CUI Registry, its purpose, structure, and location, defined in 32 CFR Part 2002.4

The CUI Registry is the authoritative resource for Government customers to identify what is CUI. The registry serves as a central repository for all information, guidance, policy and requirements for handling CUI that the Executive Branch protects. It 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. DOD agency personnel and contractors should first consult the DOD CUI Registry to find the Indexes and Categories used to identify the various types of DOD CUI. It is located at https://www.archives.gov/cui. The DOD CUI Registry is built on the ISOO Registry with the addition of the DOD issuance alignment. The authority in DOD Directive (DODD) 5143.02 and the December 22, 2010 Deputy Secretary of Defense Memorandum establishes that agencies and authorized holders with DOD Contracts are also required to follow the official DOD CUI Registry (https://www.dodcui.mil/Home/DoD-CUI-Registry/). If you are unsure the information qualifies as CUI, refer back to contract documentation and your security manager.

6. Address CUI marking requirements, as described by agency policy

CUI Registry: https://www.archives.gov/cui/registry/category-marking-list.
Download templates from the CUI Registry at: www.archives.gov/cui/additional-tools.

Marking of CUI documents is required in order to show that the document contains sensitive information. The originator of a document is responsible for determining at origination whether the information may qualify for CUI status, and if so, for applying the appropriate CUI markings. However, this responsibility does not preclude competent authority (e.g., officials higher in chain of command; functional experts) from modifying the marking(s) applied or originally applying additional markings. In such cases, the originator shall be notified of the changes. The primary marking for all CUI is the mandatory CUI Banner Marking that appears at the top of each page of any document that contains CUI. For more information on how to mark CUI, please refer to the DOD CUI Marking Job Aid located on the DCSA CUI website or the CDSE CUI toolkit at https://www.cdse.edu/toolkits/cui/current.html.

7. Address the required physical safeguards and methods for protecting CUI, as described by agency policy

Safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders. Safeguarding measures authorized or accredited for classified information and national security system are also sufficient for safeguarding CUI. Authorized holders must comply with policy in the Order, 32 CFR2002 and the DoD Registry and must safeguard CUI using one of the following types of standards: CUI Basic or CUI Specified in accordance with the CUI Registry.

For information systems, the basic system and network configuration is moderate confidentiality in accordance with the NIST Special Publication 800-171 Rev 2 (Non-Federal Systems) and the NIST Special Publication 800-53 Rev. 4 (Federal Systems).

8. Address the destruction requirements and methods, as described by agency policy

Two approved methods for destroying CUI are cross-cut shredding or pulverizing (look at DODM 5200.01-V3, February 24, 2012 and CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form via single and multi-step methods). Shredders and shredding services must comply with NIST 800-88. Destroy to 1mm x 5mm particles.

- CUI documents and materials will be formally reviewed in accordance with Paragraphs 4.5.a. and 4.5.b. before approved disposition authorities are applied, including destruction. Media containing CUI must include decontrolling indicators.
- Record and non-record copies of CUI documents will be disposed of in accordance with Chapter 33 of Title 44, U.S.C. and the DOD Components' records management directives.
- Record and non-record CUI documents may be destroyed by means approved for destroying classified information or by any other means making it unreadable.

9. Address the incident reporting procedures, as described by agency policy

Incidents involving the loss or improper safeguarding of CUI have a direct impact on national security and must be reported immediately to the contractor's security office and the facility security officer (FSO). No formal security inquiry or investigation is required unless disciplinary action will be taken against the individual(s) responsible. In such cases, a preliminary inquiry is appropriate. UD of certain CUI, such as export controlled-technical data, may also potentially result in civil and criminal sanctions against responsible persons based on the procedures codified in the relevant law, regulation, or government-wide policy. The DOD Component originating the CUI will be informed of any UD. (DODI 5200.48/ 3.9 d)

Recommend working with your security manager, GCA and DCSA IS Representative to notify applicable DOD Components about unauthorized disclosures.

The DITMAC/UDPMO determines the category of violation.

a). Tier I - no further inquiry is recommended;

b). Tier II - an internal investigation is needed; or,

c). Tier III – a criminal investigation from DOJ is needed. If the Component's inquiry confirms that further inquiry is warranted, the DOD conducts an internal investigation and takes further action by requesting criminal investigation from DOJ or notifies DITMAC/UDPMO of no further action.

10. Address the methods and practices for properly sharing or disseminating CUI within the agency and with external entities inside and outside the Executive branch; and (CUI Notice 2018-07 – CUI Limited Dissemination Controls 11/16/2018.)

The standard for sharing and having access to CUI is an authorized "lawful government purpose," meaning sharing and dissemination are only permitted when doing so complies with the law, regulation, or govern-wide policy identifying the information as CUI, furthers a lawful government purpose and is not restricted by an authorized Limited Dissemination Control (LDC) established by the CUI EA. Prior to sharing CUI, it must be properly marked to alert the user to the presence of CUI (e.g. Mandatory banner markings).

- CUI sent via email must be encrypted and transmitted electronically via approved secure communication systems.
- Packages and envelopes must be addressed to a specific recipient (with no markings of CUI on the outside of the package or envelope) and tracked.
- Facsimiles may be transmitted only if appropriate protection will be available at the receiving location (a controlled Government environment).
- The agency of designation indicator is stated on the first page or cover of all documents containing CUI.

The ability of individuals or organizations to provide adequate security for CUI must be ascertained prior to dissemination. This means that the individual processing CUI must ensure that the receiving individuals or organizations are authorized to receive CUI and have information systems or manual processes and facilities that will provide adequate security prior to transmitting CUI information. This applies both to electronic and physical dissemination.

11. Address the methods and practices for properly decontrolling CUI, as described by agency policy

The CUI program (32 CFR 2002.4(s)) explicitly defines decontrolling CUI as the removal of safeguarding or dissemination controls from CUI that no longer requires controls. The capability to decontrol CUI (both CUI Basic and CUI Specified), and to remove Limited Dissemination Controls (applied to promote a Lawful Government Purpose in handling CUI), belongs to the authorized holders. This includes the original designating agency, other Executive branch agencies and, where provided in a contract or agreement, non-federal entities.

CONTROLLED
UNCLASSIFIED
INFORMATION

FOR MORE INFORMATION:

Contact Your Local Industrial Security Representative or
the DCSA Enterprise Security Operations CUI Mailbox at:
dcsa.quantico.ctp.mbx.eso-cui@mail.mil