What is Controlled Unclassified Information?

Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and Government-wide policies but is not classified under Executive Order 13526 “Classified National Security Information” or the Atomic Energy Act, as amended.

Identifying CUI

CUI is NOT classified information and may only be marked as CUI if it belongs to a category established in the ISOO and/or DOD CUI Registry.

The CUI Registries

ISOO maintains the National CUI Registry
» https://www.archives.gov/cui
The DOD CUI Registry
» https://www.dodcui.mil

What are examples of CUI?

CUI includes, but is not limited to, Controlled Technical Information (CTI), Personally Identifiable Information (PII), Protected Health Information (PHI), financial information, personal or payroll information, and operational information.

Controlled Technical Information (CTI)

Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog item identifications, data sets, studies and analyses and related information, and computer software executable code and source code. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, “Distribution Statements of Technical Documents.”

Export Controlled Information

DODI 2040.02 states “Dual-use and defense-related technology will be treated as a valuable national security resource, to be protected and transferred only in accordance with export control laws and regulations, and national security and foreign policy objectives.”

» United States Code, Title 22, Chapter 39
• Arms Export Control
» Code of Federal Regulations, Title 22, Chapter 1, Subchapter M
• International Traffic in Arms Regulations
» Code of Federal Regulations, Title 15, Subtitle B, Chapter XI, Subchapter C
• Export Administration Regulations

CONTROLLED UNCLASSIFIED INFORMATION
Steps to Identifying CUI

START

Does the information meet the standards for classification in accordance with DODM 5200.01 Volume 1?

YES

NO

Does the information fall within a law, regulation, or government-wide policy?

YES

NO

Identify the category(s) the information falls within

DDM CUI Registry

https://public.dod.mil

This category cannot be marked as CUI

YES

NO

The CUI category is annotated on the document in the CUI Designation Indicator block

STOP

Example

Controlled By: [Name of DOD Component] [Name of Office] [PI and (xxx) xxx-xxxx]

Controlled By: [Name of Office ]

CUI Category: [Name of Office] [Name of DOD Component] [Confidentiality impact value]

Limited Dissemination Control (LDC): [Name of Office] [Name of DOD Component] [Confidentiality impact value]

Marking CUI

BANNER MARKINGS

The mandatory marking for all DOD CUI is the CUI Banner/Footer with the CUI Designation Indicator (DI) Block. This is the main marking that appears at the top and bottom of all documents containing CUI. The Banner/Footer markings must appear as bold capitalized text and be centered across the width of the page. The first page only and should include the following:

Controlled By: [Name of Office] [Name of DOD Component] [Confidentiality impact value]

Controlled By: [Name of Office]

CUI Category: [Name of Office] [Name of DOD Component] [Confidentiality impact value]

Limited Dissemination Control (LDC): [Name of Office] [Name of DOD Component] [Confidentiality impact value]

MARKING CUI

All documents containing CUI must have a CUI Designation Indicator (DI) Block to notify the reader about the confidentiality level. This is the CUI marking that contains the following information:

Controlled By: [Name of DOD Component] [Name of Office] [Confidentiality impact value]

Controlled By: [Name of Office]

CUI Category: [Name of Office] [Name of DOD Component] [Confidentiality impact value]

Limited Dissemination Control (LDC): [Name of Office] [Name of DOD Component] [Confidentiality impact value]

Sharing/Transmitting CUI

DISSEMINATION & DISTRIBUTION

No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose. CUI information may be disseminated between the DOD Components and between DOD Component officials and DOD contractors, consultants, and grantees to conduct official business for the DOD, provided dissemination is consistent with controls imposed by a distribution statement or limited dissemination controls (LDC). CUI designated information may be disseminated to a foreign recipient in order to conduct official business for the DOD, provided the dissemination has been approved by a disclosure authority in accordance with DODM 5200.01, Paragraph 3.4.a; and the CUI is appropriately marked as releasable to the intended foreign recipient.

Mailing CUI

1. Address the interior envelope/package to a specific recipient (not to an office or an organization).

2. Do not put CUI markings on the outer layer of the envelope/package.

3. Use automated tracking on the package to ensure it was delivered to the correct recipient.

4. The following methods may be used to mail/handle CUI:
   - U.S. Postal Service (USPS)
   - Any commercial delivery service (FedEx, UPS)
   - Interoffice mail delivery/Interagency mail delivery

Faxing CUI

The sender is responsible for determining appropriate safeguards in place on the receiving end of the fax and that the fax machine is located in a controlled environment. A fax cover sheet is required indicating the presence of CUI.

Protecting CUI

1. Be aware of your surroundings and take steps so that others can’t overhear what you are saying – do not use wireless phones to communicate.

2. Protect or safeguard your surroundings to prevent shoulder-surfing. Don’t allow CUI to be viewed by unauthorized individuals while you are with CUI documents printed out or displayed on a screen.

CUI Self-Inspection Program

An agency Self-Inspection Program is required to internally manage and ensure compliance with the CUI Program.

A Self-Inspection Program evaluates:

- How you are complying with the requirements for protecting, marking, storing, transporting, and destroying CUI.

If you are reporting UDs of CUI and submitting required reports:

- And if training is carried out as required.

- And if there are management oversight in place.

CUI Self-Inspection will also allow you to determine best practices, lessons learned, and to take corrective actions where necessary.

Sharing CUI

Self-Inspection will also allow you to determine best practices, lessons learned, and to take corrective actions where necessary.

Storing/Transporting CUI

CUI must be stored in controlled environments that prevent or detect unauthorized access. Printed CUI documents must be protected by at least one physical barrier, such as a cover sheet or a locked bindervault.

CUI may only be digitally stored in an authorized IT system/application provided it:

- Is configured at no less than the Moderate Confidentiality impact value.

- Has limited access based on need, and

- Meets the requirements of DOD’s IT Security Policy.

Protecting CUI

You should notify the security manager by email or through some other means (sign-out sheets) of the removal of CUI from the work environment.

Storing CUI

CUI must be stored at all times. Include having the Information Security Oversight Office (ISOO), the CUI Executive Agent, approved CUI markings on printed pages, and/or a CUI cover sheet to clearly identify the information as CUI when stored, transported, or when being used.

Placing a CUI marked document in a briefcase is acceptable for transport. There still should be one layer of protection (cover sheet, folder, or envelope) on the document.

You should notify the security manager by email or through some other means (sign-out sheets) of the removal of CUI from the work environment.

Confidentiality impact value,