

Office of the Under Secretary of
Defense for Intelligence and Security
OUSD (I&S)

Appropriate Use of Controlled Unclassified Information in the Department of Defense



CLEARED
For Open Publication

May 22, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

SLIDES ONLY

NO SCRIPT PROVIDED

24-P-0694



Background

- Explanatory Statement Regarding H.R. 2617, the Consolidated Appropriations Act, 2023 (Public Law No: 117-328) requests the Deputy Secretary of Defense to:
 - “Review the current usage of [controlled classified information] CUI to ensure its appropriate application;” and,
 - “Brief the congressional defense committees not later than 30 days after the enactment of this Act on the findings of this review.”
- To meet this requirement, OUSD(I&S) developed a survey and requested all Components provide input.



CUI Background

- Executive Order 13556 created the controlled unclassified information (CUI) program, and 32 CFR Part 2002 provides direction for its implementation.
- In March 2020, the Under Secretary of Defense for Intelligence and Security issued Department of Defense (DoD) Instruction 5200.48, "Controlled Unclassified Information," which implements and outlines DoD's policies on content that qualifies as CUI.
- The Department is participating in the National Security Council (NSC) Staff's review of the Executive Branch's information security policies.



CUI Background

- Why is CUI required?
 - CUI is a cornerstone of DoD information security requirements.
 - Adversaries and strategic competitors target DoD information in the areas where it is most vulnerable – off DoD networks.
 - CUI is the best available tool to require safeguarding requirements on non-federal systems (e.g., industry) through contractual requirements.



Summary of Findings

Key findings from the review of DoD's Controlled Unclassified Information (CUI) program.

- The Department did not identify systematic over-control of information, but understands training and oversight is necessary to ensure DoD controls only what it must in a standard and repeatable manner.
- DoD distributed training and awareness products that specifically target overapplication of CUI and sharing with Congress, the Defense Industrial Base, and foreign partners, as well as Departments and Agencies that have not implemented the Executive Order or associated Code of Federal Regulations.
- DoD training and awareness products include infographics on "CUI Basics for Congress" and "CUI: Protecting AND Sharing it," which provide clear and concise guidance for sharing CUI and include an outlet for users to pose questions to their information security subject matter experts.



DoD Usage of Controlled Unclassified Information

DoD has been the leader in implementing the CUI program, which includes the development of a comprehensive web page.

<https://www.dodcui.mil>

Mar – July 2023 Data

25,000+ visits to the Registry

45,000+ visits to the Training page

200+ inquiries utilizing the
“Contact Us” link

The screenshot shows the DoD CUI PROGRAM website. At the top left is the DoD Intelligence and Security seal. The main header reads "DoD CUI PROGRAM" with a search bar on the right. A navigation menu includes: HOME, ABOUT US, CONTACT, CMIC, WHAT'S NEW, FREQUENTLY ASKED QUESTIONS, CUI REGISTRY CHANGE LOG, and CUI REGISTRY NEW. A left sidebar contains buttons for: CUI Registry (with a red "New!" tag), Policies & Forms, Training Resources, What's New, FAQs, and Contact Us. The main content area features a "Controlled Unclassified Information (CUI)" section with a definition, a note that not all categories are applicable to DoD, and a "Why is CUI important?" section with bullet points. At the bottom, there is a "DoD Infographics" section with three links: "CUI Basics for Congress", "CUI Basics for Congress FAQs", and "CUI Basics for DoD Personnel".



DoDI 5200.48 implements E.O. 13556 and 32 CFR Part 2002 and provides guidance to DoD personnel on implementation of the CUI program.

DoD policy memoranda provide guidance and clarification on CUI policies.

DoD CUI training instructs personnel on how to use the website and CUI Registry (next slide).

The DoD CUI website includes a Policy & Forms web page:

- Federal-level policy
- DoD-level policy and memoranda-Related policies
- CUI cover sheet

CUI Policies

Executive Order 13556
Controlled Unclassified Information
This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

32 Code of Federal Regulations, Part 2002
Controlled Unclassified Information
The implementing directive describes the executive branch's Controlled Unclassified Information (CUI) Program (the CUI Program) and establishes policy for designating, handling, and decontrolling information that qualifies as CUI.


DoD Instruction 5200.48
Controlled Unclassified Information (CUI)
Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012.

Related Policies

DoD Instruction 5230.24
Distribution Statements on DoD Technical Information
Establishes a standard framework and markings for managing, sharing, safeguarding, and distributing technical information in accordance with national and operational security, privacy, records management, intellectual property, Federal procurement, and export-control policies, regulations, and laws.

DoD Information Security Policies

Forms



SF 901

CUI Policy Memorandums

Authorized Telework Capabilities, 20200413

Clarification to Controlled Unclassified Information Policy Regarding Disclosures to Members of Foreign Governments, 20211129

Clarifying Guidance for Marking and Handling CTI, 20210321

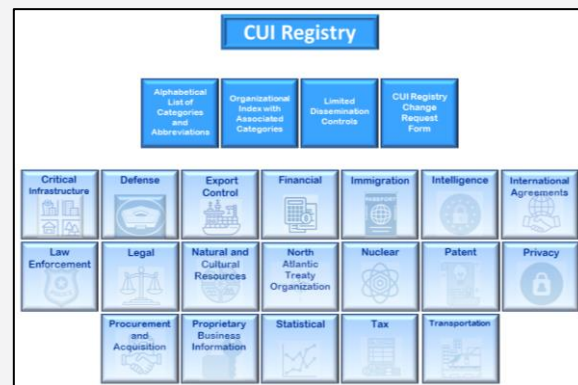
Use of Non-Government Owned Mobile Devices, 20220803



Using the CUI Registry

The DoD CUI website also hosts the DoD CUI Registry.

- The DoD CUI Registry is available for users to determine whether information is CUI and the appropriate CUI category to apply.
- The organizational index groups categories of information.
- Each category has its own page and includes information about the category, examples of the type of information that falls in each category, and the statute(s), regulation(s), or government-wide policy that authorizes the controlling of such information.
- Under each organizational index group is a list of categories.
- Each category has a separate page with detailed information.



CRITICAL INFRASTRUCTURE

Categories

- Ammonium Nitrate
- Chemical-Terrorism Vulnerability Information
- Critical Energy Infrastructure Information
- Emergency Management
- General Critical Infrastructure Information
- Information Systems Vulnerability Information
- Physical Security
- Protected Critical Infrastructure Information
- SAFETY Act Information
- Toxic Substances
- Water Assessments

Critical Energy Infrastructure Information

Category Abbreviation:
CEII

Category Description:
Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (i) Relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure,... and (iii) Does not simply give the general location of the critical infrastructure.

Required Warning Statement:

Required Dissemination Control:

[Back to Main Page](#)

[CUI Registry](#)

Quick Links to Critical Infrastructure Categories

- Ammonium Nitrate
- Chemical-Terrorism Vulnerability Information
- Emergency Management
- General Critical Infrastructure Information
- Information Systems Vulnerability Information
- Physical Security
- Protected Critical Infrastructure Information
- SAFETY Act Information
- Toxic Substances
- Water Assessments

Examples

National Authorities

DoD Authorities

- Electrical distribution system
- FCAS builds/layouts
- Sub stations
- Power grids
- HVAC

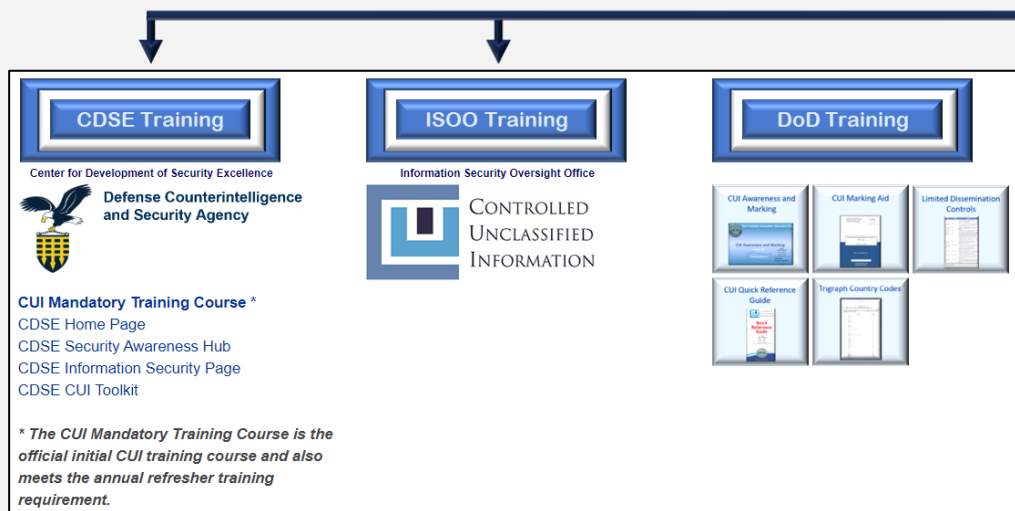
18 CFR 388.113



DoD CUI Training

The DoD CUI website hosts DoD CUI training products and links to CUI training hosted by the Center for the Development of Security Excellence (CDSE) and the NARA Information Security Oversight Office (ISOO).

- In addition to the mandatory training course, Information Security Managers conduct group, one-on-one, and ad hoc CUI training sessions, using attendees' current work products and question-and-answer sessions.
- Security Managers leverage teachable moments during draft document reviews; pre-publication document reviews; and CUI challenges.



The web page contains links to the Information Security Oversight Office training site and to the official DoD training website.

It also provide DoD-specific training aids.

Along with the mandatory annual training, DoD Components conduct group and one-on-one training sessions using current work products.



DoD CUI Contact Page

It is easy for people (both internal and external to the Department) to ask questions about the Department's CUI program.

Individuals are encouraged to submit their questions to OUSD(I&S) directly using the **Contact Us** link and usually get a response the same day.

- CUI Registry **New!**
- Policies & Forms
- Training Resources
- What's New
- FAQs
- Contact Us



Contact Form

Contacts

- DoD INFOSEC Mailbox

Recipient:
Choose a Recipient


Your Name:

Your Email Address:

Subject:

Message:

Contact Me: A response is requested.

I'm not a robot  reCAPTCHA
Privacy - Terms

The CUI website also includes POCs for CUI programs throughout the Department, allowing users to reach out directly to the most relevant office for their question.



DoD CUI Frequently Asked Questions

- CUI Registry **New!**
- Policies & Forms
- Training Resources
- What's New
- FAQs
- Contact Us



Frequently Asked Questions

Privacy/PII

Is my CAC CUI because it contains the DoD ID number (EDIP)?

No. While the DoD ID number is personally identifiable information (PII), it does not meet the criteria for CUI unless it is included in a grouping of information that contains the individual's name or other unique identifier combined with one or more of the following:

- Truncated SSN (such as last four digits)
- Date of birth (month, day, and year)
- Citizenship or immigration status
- Ethnic or religious affiliation
- Sexual orientation
- Criminal history
- Medical information
- System authentication information such as mother's maiden name, account passwords, or personal identification numbers

I have a document that contains PII. Do I have to mark it as CUI?

Not necessarily. It depends on what PII is on the document. Examples of PII include social security number, passport number, driver's license number, taxpayer identification number, patient identification number, financial account or credit card number, personal address and phone number, biometric records. The document becomes CUI when individual pieces of PII are combined which can then be used collaboratively to identify a specific individual.

When do I need to put a Privacy Act Statement (PAS) on a document?

When a Federal agency requests that you provide personal information (name, date of birth, social security number, etc) for a system of records, regardless of the method used to collect the information (i.e., forms, personal or telephonic interview, etc), a Privacy Act Statement (PAS) is required. If the information requested will not be included in a system of records, a PAS is not required.

Distribution Statements

We were told to put a distribution statement on a document, but there is no CUI in the document. Can a document have a distribution statement and not be CUI?

The application of a distribution statement does not automatically mean the document is CUI. Do not confuse the two issues. Pursuant to DoDI 5230.24, "Distribution Statements on DoD Technical Information," distribution statements are applied to technical documents, regardless of whether the document is classified, unclassified, or CUI. Certain CUI categories require a distribution statement because of the technical nature of the information. Not every document containing CUI requires a distribution statement.

Information Sharing

Can we share CUI with Congress?

Yes. It is DoD policy to provide Congress with all the information it needs to conduct effective oversight. Any Member of Congress and their personal or professional staff are authorized to receive and share CUI from DoD.

Can I share CUI with foreign allies and partners?

Yes, you may share CUI with our foreign allies and partners unless sharing with that country is specifically restricted.

The DoD CUI webpage includes a Frequently Asked Question's (FAQ) section informed by questions from many different stakeholders, including Military Personnel and Civilians, Industry, Academia, and the public.



Facilitating Information Sharing with Congress

The main page of the DoD CUI website includes links to three different resources that inform members of the department on the basics of sharing CUI, including with members of Congress.

In addition to being available on the DoD CUI website these materials were:

- Distributed to DoD Components
- Briefed during CUI training, Action Officer courses, and security conferences

DCP/PS 23-5-1408

CLEARED For Open Publication Apr 17, 2023

CUI BASICS FOR CONGRESS

Department of Defense Office of Information Security

CUI is unclassified information that requires safeguarding or dissemination controls —

What is CUI?

- Controlled Unclassified Information (CUI) is unclassified information the United States Government creates or possesses that requires safeguarding or dissemination controls (beyond its distribution to those with a lawful government purpose). CUI may not be released to the public absent further review.
- The DoD CUI Program, established through Executive Order 13526, standardizes the safeguarding of information across multiple categories. For example, CUI categories exist to protect Privacy Act information, attorney-client privileged information, and controlled technical information, among many others. A complete list of these categories is available at the DoD CUI Registry found at <https://www.dodcui.mil>.
- CUI markings alert recipients that special handling may be required to comply with law, regulation, or government-wide policy.
- For DoD, CUI also enables consistent processes to safeguard information for specific national security purposes, such as physical and operations security.
- CUI-protected information is unclassified, but requires control to prevent release of unclassified information that, if publicly associated with sensitive missions or aggregated with other sources of information, often will reveal exploitable information to adversaries or violate statutory requirements.

Who can access CUI?

- Any Member of Congress and personal or professional staff are authorized to receive and share CUI from DoD.
- The standard for access to CUI is a "lawful government purpose." This is defined as "any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of a non-executive branch entity" (52 CFR 2002.2-6(b)).
- Many different groups may have a "lawful government purpose" to receive access to CUI. In addition to any Member of Congress or their staff, this may include State, Local, Tribal and Territorial Governments, appropriate industrial partners, other Federal Agencies, Allies and Partner nations, and members of academia.

How should members and staff handle CUI?

- If a document is marked CUI and provided to members or staff, either during a briefing or otherwise, it can be shared widely. CUI does not prohibit dissemination within Congress — only prohibits public release.
- CUI markings do not prohibit Executive Branch briefers from leaving documents behind after a congressional engagement.
- Members and staff can request to keep any materials brought to a briefing.

What do the markings "Legislative Materials" and "For Committee Use Only" mean?

- The CUI category "Legislative Materials" (LMI) is applied to protect data related to Congress's legislative or oversight responsibilities over DoD. This includes data related to proposed or pending legislation as well as DoD responses to Congressional requests and any other information which, if disclosed, would reveal the nature and scope of congressional inquiries to DoD.
- "For Committee Use Only" indicates that only Members and staff of a particular Committee should read a document. DoD recognizes there may be a need to share information beyond the Committee. When this is necessary, DoD asks that the Committee recontact with DoD to see if DoD can help remove that requested information where possible.
- For example, in extraordinary circumstances personally identifiable information (PII) may be provided in response to congressional investigation where PII is requested in a Chairman's letter. In such cases, any production involving PII would be for Committee Use Only.

What actions is the Department taking to educate and implement proper use of CUI with Congress and internal to the Department?

- DoD requires annual CUI training. To date, 2.3 million military, civilian and contractor personnel have been trained. Training resources are available at <https://www.dodcui.mil>.
- DoD is taking steps to reform its congressional reporting processes so that unclassified reports are written with the expectation of public release. Reports which require inclusion of CUI, or other non-public information, will be included as an annex.
- DoD's program is an implementation of existing federal requirements. The Department is a leading advocate for increased simplification and uniform adoption by all federal agencies of the national CUI program through an ongoing interagency review process.

May share within Congress

DoD's disclosure to public without further review

Markings protect data related to Congress's DoD coverage

LMI

"For Committee Use Only" is NOT CUI

CUI annual training required

Stay tuned! More programs and processes to come

FOR MORE INFORMATION, VISIT <https://www.dodcui.mil>

DoD Infographics

- CUI Basics for Congress
- CUI Basics for Congress FAQs
- CUI Basics for DoD Personnel

DCP/PS 23-5-1408

CLEARED For Open Publication Apr 06, 2023

CUI: PROTECTING IT AND SHARING IT

Department of Defense Office of Information Security

"Not exactly. CUI is unclassified information that a law, regulation, or government-wide policy requires safeguarding or dissemination controls."

"This is just the new FOIA, right?"

"Although DoD transitioned to CUI, not all Federal agencies have Documents with other markings (e.g. FOUO, SRU) should be handled in accordance with guidance from those agencies."

"Information covered under the Privacy Act or Export Control?"

"Give me an example or two of those?"

"Should I be encrypting CUI emails?"

"Yes! CUI is more than markings! It's about safeguarding."

"What about allies and partners?"

"Yes, you may share CUI with allies and partners, unless sharing with that country is specifically restricted."

"Should I share CUI with Congress?"

"Yes! It is DoD policy to provide Congress with all the information it needs to conduct effective oversight. This includes CUI marked FEDCON and FEDCOM."

"How can I learn more about CUI?"

"Who can I go to when I have questions about CUI?"

"Go to the DoD CUI website (dodcui.mil) where you can find the CUI Registry, get alerts, the CUI Registry, or submit inquiries!"

"Each Component has a CUI Program Manager. If you don't know who that is, contact your CUI Liaison (dodcui.mil) and we'll get you to them."

FOR MORE INFORMATION, VISIT <https://www.dodcui.mil>



CUI and Security Classification Guides (SCGs)

To facilitate the appropriate use of CUI, DoD requires CUI elements of information be identified in SCGs. SCGs are used by the Department to identify classified and unclassified information within a system, plan, program, project, or mission. DoD Components provide guidance on the importance of identifying information designated as CUI in an SCG to ensure that derivative classifiers continue to designate information appropriately identified as CUI.

DoD is in the process of updating DoD Manual 5200.45, "Original Classification Authority and Writing a Security Classification Guide."



CUI Document Reviews

DoD has various processes and procedures to check on the markings of CUI documents.

- DoD Components have dedicated security professionals and Staff Action Control Offices that review correspondence for appropriate CUI banners, designation indicators, and portion markings prior to distribution.
- Additionally, the Department of the Army has ensured command emphasis through the Office of the Deputy Chief of Staff, G-2, Controlled Unclassified Information Guidelines, stating that management of CUI will be incorporated in a command's Information Security program.
- The Department of the Air Force (DAF) also requires all DAF activities to complete a CUI self-assessment checklist via the Air Force Management Internal Control Toolset (MICT) on an annual basis to assess program implementation, which includes an assessment of CUI document marking.

OUSD(I&S) has directed DoD Components to assess documents marked CUI as part of this review.

- No documents were discovered to be inappropriately marked as CUI. However, in some instances an incorrect CUI category was applied.
- Some documents had other marking issues, such as a lack of designation indicator blocks, that were corrected through the staff action process.



Overall Assessment of DoD CUI Program

As DoD continues to work through the implementation of CUI, OUSD(I&S) assesses the overall DoD CUI program is strong.

Training continues to be updated as required to help close knowledge gaps.

The CUI web page continues to be the primary source of information on CUI categories, policy, and training material. The web page is continually updated to ensure the latest information is available.

DoD continues to collaborate across the Executive Branch to synchronize CUI practices.