



CONTROLLED
UNCLASSIFIED
INFORMATION

QUICK START GUIDE FOR INDUSTRY



WHY THIS GUIDE?

Safeguarding Controlled Unclassified Information (CUI) is a Department of Defense (DOD) requirement and a key tool for the protection of sensitive, unclassified information. This guide provides basic facts for industry, answers frequently asked questions, and provides sources of more detailed information and tools.

CONTENTS

3 CUI Overview

What is CUI? ... 3

CUI Implementation Timelines ... 4 CUI
and the CMMC Framework ... 4

DCSA's Roles and Responsibilities ... 4

CUI Lifecycle ... 5

CUI Marking Guidelines, Categories,
and Registries ... 6

CUI Transmittal ... 6

7 Frequently Asked Questions

8 Where to Learn More

Governing Documents ... 8

CUI Training ... 8

Other Resources ... 8



CUI OVERVIEW

WHAT IS THE CUI PROGRAM?

The CUI Program is a safeguarding system for the protection of unclassified information. Although this information is not considered “U.S Government classified,” it is still sensitive and important, and requires protection. The CUI Program standardizes the way the Executive Branch handles unclassified information that does not meet the criteria required for classification under E.O. 13526, “Classified National Security Information,” December 29, 2009, or the Atomic Energy Act. However, law, regulation, or government-wide policy still mandates protection for this unclassified information. That protection involves safeguards employed while CUI is being stored or handled by the Executive branch departments

or agencies as well as the controls involving how the information is disseminated.

CUI is information that is created or owned by, or on behalf of, the government. CUI is not a classification and should not be referred to as “classified as CUI.” A better way to phrase it is “designated as CUI.” CUI is not corporate intellectual property, unless created for or included in requirements related to a Government contract. Contractors should consult with their Government Contracting Activity (GCA) to make this determination. In some cases, CUI designations replace For Official Use Only (FOUO) and Sensitive but Unclassified (SBU) designations.

CUI is not a classification and should not be referred to as “classified as CUI.” A better way to phrase it is “designated as CUI.”



CUI IMPLEMENTATION TIMELINES

CUI is a government-wide directive mandated by Executive Order 13556 and impacts more than 100 departments and agencies within the Executive branch. As each department and agency is in process of developing their CUI program and updating their contracts to include CUI requirements, Industry may receive new contractual CUI requirements at different times. Industry is encouraged to work with its Government Contracting Activities to further understand CUI requirements and implementation timelines.

The DOD CUI Program was directed by DoDI 5200.48 on March 6, 2020. As such, Industry partners with active DOD contracts or those planning to bid on future contracts must be familiar with CUI requirements and have a plan to address them.

CUI AND THE CMMC FRAMEWORK

The Cybersecurity Maturity Model Certification (CMMC) is a unifying standard for the implementation of cybersecurity controls across the Defense Industrial Base (DIB). The CMMC framework includes

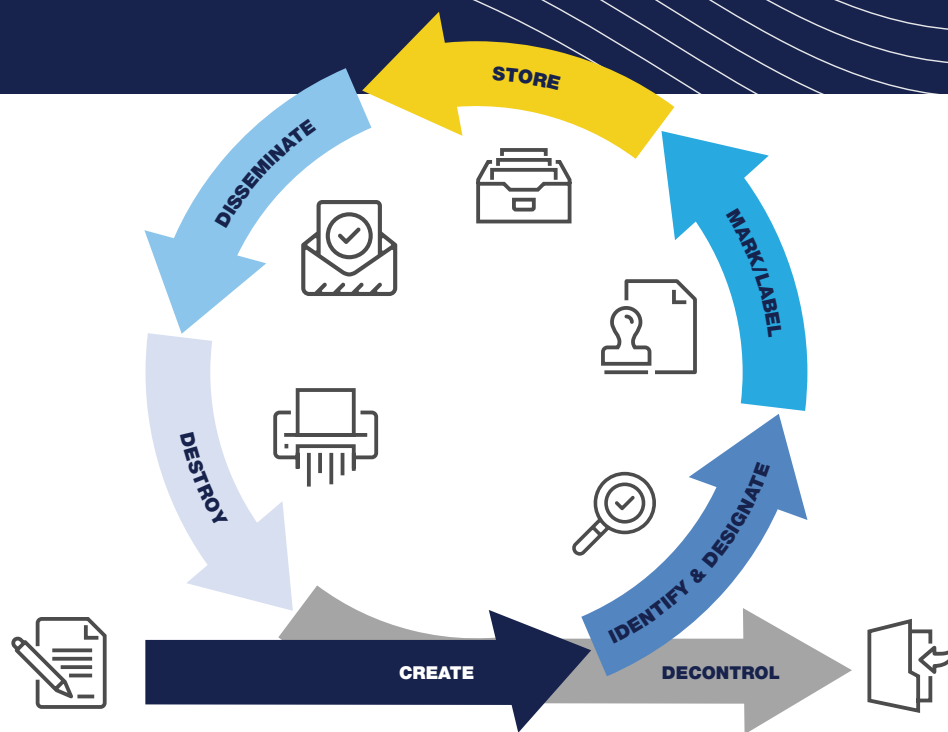
a comprehensive and scalable third-party certification element to validate the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to agencies that a Defense Industrial Base (DIB) company can adequately protect sensitive information including CUI, accounting for information flow down to subcontractors in a multi-tier supply chain.

DCSA'S ROLES AND RESPONSIBILITIES

DoD Instruction 5200.48 directed DCSA with eight responsibilities related to CUI. DCSA's Critical Technology Protection (CTP), Enterprise Security Operations (ESO) office is leading efforts to provide logical and efficient administration of the CUI Program. DCSA will be executing its responsibilities in a deliberate and phased approach over multiple years and will keep industry informed on its progression.

In Phase 1, DCSA will be focusing on security education and training, development of processes, and establishment of the CUI Program Office. DCSA is not currently conducting assessments of CUI oversight for programs associated with classified contracts and cleared contractors but will include CUI compliance as an element of security reviews in the future.

Right now, Industry should review existing contracts and engage with Government Contracting Activities to determine which, if any, CUI requirements are applicable to current contracts and the appropriate way forward.



CUI LIFECYCLE

CUI follows a lifecycle similar to all protected information. While the designation of certain types of information requiring safeguarding and dissemination may be new, the process should be very familiar to Industry partners.

- **Create:** CUI is created when put on paper or entered into an information system.
- **Identify & Designate:** Realize that the information is generated for or on behalf of an agency within the Executive Branch under a contract and determine if the information falls into one of the more than one hundred categories of CUI in the National CUI Registry. It is also important to realize what is not CUI.
- **Mark/Label:** At minimum, CUI markings for unclassified DOD documents will include the acronym “CUI” or “CONTROLLED” in the banner of the document. It is a best practice to include markings in both the banner and footer of the document, and it is imperative to reference the CUI Marking Guide to ensure correct markings.
- **Store:** CUI can be stored in NIST 800-171 compliant information systems or controlled physical environments.
- **Disseminate:** Only authorized holders may disseminate in accordance with distribution statements, dissemination controls, and applicable laws.
- **Destroy:** Hard and soft copies of CUI should be appropriately destroyed, meaning they are rendered unreadable, indecipherable, and irrecoverable. Review clearing, purging, and destruction in NIST SP 800-88: Guidelines for Media Sanitization.
- **Decontrol:** All holders must promptly decontrol CUI once the CUI owner has properly determined the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy in accordance with DoDI 5230.09.

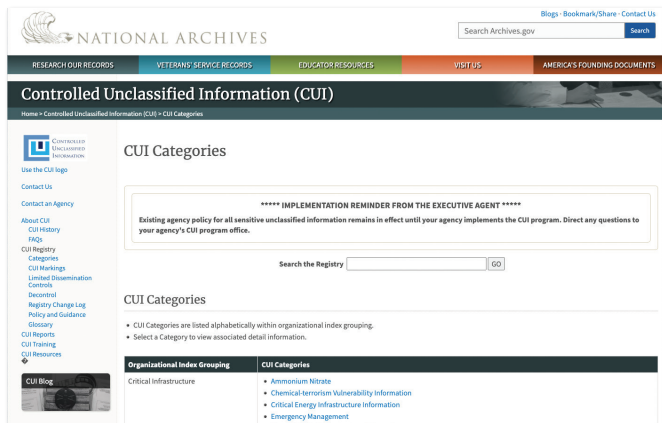


CUI MARKING GUIDELINES, CATEGORIES, AND REGISTRIES

Limited Dissemination Control (LDC) markings are used to limit and/or control who can or cannot access the CUI. "CUI" replaces legacy markings in header, footer, and portion markings. Marking requirements apply to documents, emails, and forms of media that are designated as CUI. Remember, CUI can be found in many places including drawings (technical, schematic, design, etc.), Word documents, Excel files, PowerPoint presentations (plans and status documents), notebooks, and handwritten sticky notes. It exists in both hard copy and soft copy, on computers, and in removable storage.

CUI also includes unique categories that further restrict or direct its handling. There are two useful CUI Registries for DOD contractors providing government-approved CUI Categories and Organizational Index Groupings:

- **The National CUI Registry** is the official government-wide list of CUI indexes and categories and can be found on the National Archives and Records Administration (NARA) website.

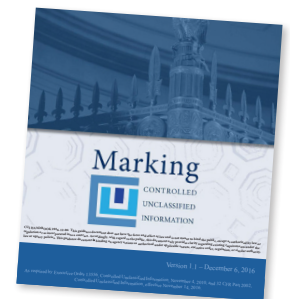


- **The DOD CUI Registry** is a resource which includes the indices and categories used to identify various types of DOD CUI. This is a helpful tool for Industry when they are contracting with the DOD, however, the official National CUI Registry contains all the indexes and categories for the entire Executive Branch. In the future, DCSA will be developing and publishing products that provide examples of utilizing the CUI Registries.

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. The DOD CUI Registry aligns each Index and Category to DOD issuances. The National CUI Registry contains Indexes and Categories for the entire Executive Branch and should be consulted for non-DOD contracts.

CUI TRANSMITTAL

CUI materials in paper or media format can be sent via first class mail, parcel post, or bulk shipments. CUI can also be transmitted by e-mail when practical, via approved encrypted communications systems, or systems using other protective measures. Please see the [DOD CUI Marking Guide](#) for details on how to mark e-mails and mail.



FREQUENTLY ASKED QUESTIONS

How will Industry know if their contracts require CUI protection, protocol, and oversight?

DOD will determine CUI requirements for each Request for Proposal (RFP) and contract to include classified and unclassified efforts. In the future, DD 254s will contain verbiage regarding CUI oversight and control requirements. For awarded contracts, Industry should review carefully and engage with their GCA to determine which, if any, CUI requirements are applicable to current contracts and the appropriate way forward. For RFPs, follow guidance provided and ask questions to ensure submissions are compliant.

What is a prime contractor's responsibility for CUI compliance with its partners?

As with most compliance matters, a prime contractor is responsible for ensuring that all teammates, including sub-contractors and suppliers meet applicable security requirements. Prime contractors should refer to Rule 32 CFR Part 117, the DoDI 5200.48 and DFARS Clause 252.204-7012 to understand their obligations and options.

What should Industry do with legacy information and materials?

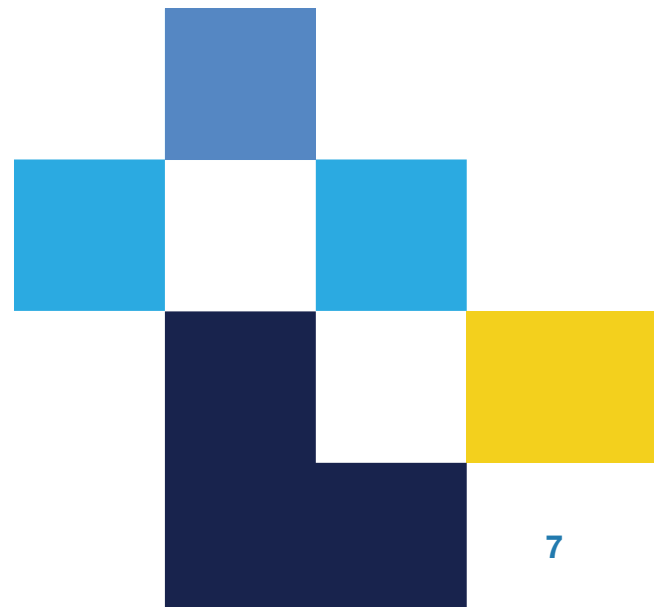
Sensitive unclassified information that was marked prior to the implementation of the CUI Program which meets the standards for CUI is considered legacy information. At a minimum, Industry should ensure it has an inventory of its current legacy information. Legacy documents do not need to be remarked unless and until the information is re-used, restated, or paraphrased. When new documents are derived from legacy documents, they must follow the new CUI marking standards.

What should Industry do if it has questions or concerns about the requirements and implementation of CUI for its existing contracts?

When contract-specific questions or concerns arise, Industry is encouraged to work with its DOD Contracting Office Representative (COR) and follow guidance issued by DOD Contracting Authority and DFARS 252.204-7012. As with all security requirements, Industry Facility Security Officers (FSOs) should ensure their organizations appropriately implement CUI requirements. Industry is encouraged to work with DCSA Industrial Security Representatives (ISRs) as appropriate.

Are FSOs expected to be experts on the CUI Program?

No, FSOs should work with their IT partners and other company subject matter experts to ensure their organizations appropriately implement CUI requirements. Their priority is to ensure company compliance with the CUI Program.





WHERE TO LEARN MORE

GOVERNING DOCUMENTS

The following policies are important for understanding and managing CUI. Be aware that in some cases the DoDI 5200.48 requirements are more stringent than the following policies. When this occurs, DOD and its Industry partners are required to follow the more stringent requirements of DoDI 5200.48.

1. **[DoDI Instruction 5200.48](#)** Controlled Unclassified Information (CUI). This Instruction establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DOD and establishes the official DOD CUI Registry.
2. **[32 CFR Part 2002](#)** “Controlled Unclassified Information.” Part 2002 establishes the CUI Program throughout the Federal Government and describes the roles, responsibilities, and key elements of the program.
3. **[E.O. 13556 Vol 75, No 216](#)**. “Controlled Unclassified Information.” The Order establishes a uniform program for managing information that requires safeguarding or dissemination controls across the Federal Government.
4. **[NIST Special Publication 800-171 Rev. 2](#)** “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.” This publication identifies the baseline CUI system security requirements for Industry established by Part 2002 of Title 32, CFR.

CUI TRAINING

Training is required when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements. **DOD contractors are required to take training**

annually per the DoDI 5200.48. Industry should note that this is *different* from the 32 CFR 2002 which requires training every two years.

The Center for Development of Security Excellence (CDSE) has CUI training available. While this training fulfills CUI training requirements, contractors have the option of developing their own training as long as it contains the mandatory 11 topics covered in [CUI Notice 2016-01](#).

OTHER RESOURCES

DOD and others in the Federal Government provide several resources and tools for Industry to better understand CUI requirements and will update them as appropriate. In addition to the policies referenced earlier, the following tools will also provide helpful information:

1. Resources on the [DCSA website](#):

- CUI Quick Reference Guide
- Critical Technology Protection (CTP) Enterprise Security Operations (ESO) CUI Information Sheet

2. Resources on the [DOD CUI website](#):

- DOD CUI Registry
- CUI Awareness and Marking Presentation
- CUI Limited Dissemination Controls
- DOD CUI Marking Aid

3. Resources on the [NARA website](#):

- National CUI Registry
- CUI Audio, Photography, and Video Markings
- CUI Destruction Label
- CUI Email Marking
- CUI Executive Agent (EA) Training Modules