CUI Guide for Defense Contractors

What You Need to Know About Controlled Unclassified Information

As a defense contractor, safeguarding Controlled Unclassified Information (CUI) is a contractual and regulatory requirement tied to frameworks such as CMMC 2.0, DFARS 252.204-7012, and NIST SP 800-171. Understanding CUI's origins, definitions, and responsibilities is critical to achieving compliance and protecting national security information.

This guide outlines the origins of the CUI program, the Department of Defense (DOD) implementation requirements, and practical expectations for contractors. While this guide is focused on DOD contractors, the principles broadly apply to contractors supporting other federal agencies—such as the Department of Energy or the Department of State—who may also flow CUI, even if their programs are less mature in implementation.

The Origins and Purpose of the CUI Program

Before 2010, federal agencies used inconsistent labels like "For Official Use Only" (FOUO) and "Sensitive Security Information" (SSI) to mark unclassified but sensitive information. This fragmented approach led to confusion and inconsistent protection.

To address this, President Barack Obama issued Executive Order 13556 in November 2010, establishing the Controlled Unclassified Information (CUI) program. The Executive Order directed:

- Standardization of safeguarding for information requiring protection under law, regulation, or government-wide policy.
- Clear distinction between CUI and classified information.
- Appointment of the National Archives and Records Administration (NARA) as the CUI Executive Agent.

NARA published 32 CFR Part 2002 to implement the Executive Order, defining policies for designating, marking, safeguarding, disseminating, and decontrolling CUI.

Key point for contractors: Only the government (e.g., DOD contracting officers or program managers) determines what information qualifies as CUI. Contractors are not authorized to independently designate CUI based on general reference materials.

Understanding the NARA and DOD CUI Registries

NARA maintains the CUI Registry, listing all government-wide categories of CUI tied to specific laws, regulations, or policies. The DOD CUI Registry refines this list for DOD-specific categories relevant to defense contracts.

While these registries are important references for understanding what CUI categories exist, they do not authorize contractors to classify or mark CUI. The government must identify CUI through contracts, markings, or explicit guidance.

How the Department of Defense Implements CUI Requirements

The DOD formalized CUI requirements through DOD Instruction 5200.48 (March 2020), which established the DOD CUI Program and outlined policies and responsibilities for the protection of CUI. The instruction:

- Defines how CUI must be marked, safeguarded, disseminated, and decontrolled within DOD and by DOD contractors.
- Clarifies the DOD’s responsibility to identify and mark CUI at the time of creation or prior to dissemination, including when sharing with contractors.
- Commits to including clear CUI markings in solicitations, contracts, and other official communications to reduce ambiguity and ensure contractors understand their safeguarding obligations.

The instruction explicitly states that it is the DOD's duty—not the contractor's—to determine whether information is CUI. This expectation helps ensure consistency in marking and clarity across the defense industrial base.

If your contract includes CUI obligations, you must protect CUI in accordance with:

- Markings and instructions provided by the government.
- Safeguarding requirements outlined in NIST SP 800-171.
- DFARS 252.204-7012 clause requirements.

However, it is widely acknowledged that DOD marking practices have historically been inconsistent. While DoDI 5200.48 represents a formal commitment to better practices, contractors should remain proactive in seeking clarification and building internal awareness of potential CUI exposures.

Where CUI Appears in Contractor Environments

While most contractors think of CUI as something received and handled under contract, CUI can and does exist outside of formal contract performance. Several business functions may engage with CUI before a contract is awarded or outside of direct program execution:

- **Business Development (BD):** May receive CUI in specifications, RFIs, or RFP attachments.
- **Contracts and Procurement**: May handle CUI during pre-award exchanges, sub-tier supplier coordination, or teaming agreements.

- **Facility Security Officers (FSOs):** Often interact with CUI systems and information, especially via DOD platforms.
- **Program Teams:** Once under contract, these roles manage, store, transmit, and collaborate on CUI throughout the performance period.

Understanding that CUI can permeate an organization before, during, and outside of delivery is essential. Protection must extend across all touchpoints—not just where the widget gets built.

What is Controlled Unclassified Information (CUI)?

CUI is unclassified information created or possessed by the government (or by a contractor on behalf of the government) that requires safeguarding or dissemination controls under applicable laws, regulations, or government-wide policies.

CUI falls into two designations:

- **CUI Basic:** Requires standard safeguarding per the CUI Registry without additional handling requirements.
- **CUI Specified:** Requires specific, enhanced safeguarding as dictated by the underlying law, regulation, or policy.

Most CUI encountered by contractors will be CUI Basic unless otherwise specified.

How to Identify and Scope CUI Within Your Organization

One of the biggest challenges defense contractors face is that the government—especially the DOD—has historically failed to consistently mark or specify CUI in contracts. Despite the issuance of DoDI 5200.48, marking practices remain inconsistent.

Because of this, contractors must go beyond simply reacting to marked data. They must:

- Determine how CUI does flow within their environment.
- Model how CUI could flow, based on contract scope, interactions, and known data pathways.
- Consider both digital and physical transmission (e.g., portals, email, removable media, physical shipments).
- Account for interactions with prime contractors, subcontractors, and teaming partners.

This approach means identifying where CUI is actively exchanged and where it could reasonably be expected to appear, even in the absence of perfect upstream clarity. Things are likely to improve as DOD enforcement matures—but in the meantime, contractor diligence must lead.

Common data types to examine include:

- **Federal Contract Information (FCI):** Non-public contract information.
- **Covered Defense Information (CDI):** Subset of CUI associated with DOD contracts.

- **CUI:** As defined by Executive Order 13556.

How to Mark and Categorize CUI Correctly

Contractors handling CUI must follow government-provided markings and instructions. When marking is missing or unclear, contractors should:

- Refer to contract clauses.
- Engage the contracting officer or program manager for clarification.

Example banner markings include:

Banner Marking	CUI Category	Group
CUI//SP-CTI	Controlled Technical Information	Defense
CUI//SP-EXPT	Export Controlled	Export Control
CUI//SP-PRVCY	Privacy	Privacy

(Refer to NARA and DOD registries for full listings.)

Protecting CUI

Once identified, CUI must be protected through:

- Defining system boundaries (System Security Plan - SSP).
- Mapping data flows to identify storage, processing, and transmission points.
- Implementing NIST SP 800-171 security controls.
- Documenting policies and procedures for CUI handling.

Avoid over-scoping by carefully identifying actual CUI data locations rather than assuming all systems handle CUI.

Key Milestones in the Evolution of CUI Requirements

- **Nov 2010:** Executive Order 13556 issued.
- **Oct 2016:** DFARS 252.204-7012 published.
- **Dec 2016:** NIST SP 800-171 Rev. 1 issued.
- **Feb 2020:** NIST SP 800-171 Rev. 2 issued.
- **Mar 2020:** DOD Instruction 5200.48 published.
- **Nov 2021:** CMMC 2.0 announced.
- **May 2024:** NIST SP 800-171 Rev. 3 published (not yet contractually required).

Required CUI Training for Defense Contractors

Mandatory CUI training is often required under government contracts that involve the handling of CUI. However, not all training resources are equally relevant for contractors. Recommended CUI training resources include:

- CDSE CUI Courses (Preferred: More directly aligned with how defense contractors are expected to handle CUI)
- NARA CUI Training
- DOD CUI Training Portal

Note: Some government-provided CUI training—particularly NARA or DOD-specific courses—may assume the user has classification authority or is operating within a government agency context. Contractors should prioritize training that aligns with their role as recipients and handlers of CUI, rather than as original classifiers or creators.

Frequently Asked Questions About CUI for Defense Contractors

Can contractors decide what information is CUI? No. Only the government determines and marks CUI.

What if CUI markings are missing? Consult your contract or contact your contracting officer.

Can registries be used to self-mark CUI? No. Registries are references for understanding categories, not for making marking decisions.

Does this only apply to DOD contractors? No. While DOD has been the primary driver of CUI maturity, these requirements apply to contractors for any federal agency that handles sensitive but unclassified information.

Conclusion: Why Proactive CUI Management Matters

Understanding and managing CUI is essential for compliance with CMMC 2.0, DFARS 252.204-7012, and NIST 800-171. By identifying, safeguarding, and properly handling CUI based on government designation, defense contractors uphold both regulatory requirements and national security obligations.

In the absence of perfect upstream clarity, contractor maturity in modeling and protecting CUI is essential. As government enforcement improves, contractors who proactively build defensible, risk-informed CUI protections will be best positioned to comply and compete.

Need help managing CUI and ensuring compliance? Reach out to a CyberSheath expert today to get the guidance and support your organization needs.