DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CONTROLLED
UNCLASSIFIED
INFORMATION

FREQUENTLY ASKED QUESTIONS (FAQs)

CONTENTS

WHAT IS CONTROLLED UNCLASSIFIED INFORMATION (CUI)? IS IT A NEW CLASSIFICATION LEVEL?

CUI is a safeguarding system for unclassified information. Although this type of information is not considered "classified," it is still sensitive, important and requires protection. CUI standardizes the way in which the Executive Branch handles unclassified information that does not meet the criteria for classification under Executive Order 13526, "Classified National Security Information," December 29, 2010, or the Atomic Energy Act. However, law, regulation, or government-wide policy still mandates protection for this unclassified information. That protection involves safeguards throughout the CUI lifecycle.

CUI is not a classification. Therefore, information cannot be "classified as CUI;" rather, this type of information is designated as CUI. In some cases, CUI designations replace For Official Use Only (FOUO) and Sensitive but Unclassified (SBU) designations and markings.

WHAT IS THE DIFFERENCE BETWEEN FEDERAL CONTRACT INFORMATION (FCI) AND CUI?

FCI is information not intended for public release. FCI is provided by or generated for the Federal Government under a contract to develop or deliver a product or service.

CUI and FCI share important similarities and a particularly important distinction. Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government. However, while FCI is any information that is "not intended for public release," CUI is information that requires safeguarding and may also be subject to dissemination controls.

In short: ***All CUI in possession of a Government contractor is FCI, but not all FCI is CUI.***

IS CORPORATE INTELLECTUAL PROPERTY CUI?

CUI is not corporate intellectual property unless created for, or included in requirements related to a government contract. This includes information and material related to or associated with the following categories when created specifically for the DOD:

- A company's products, business, or activities, including but not limited to financial information
- Data or statements
- Trade secrets
- Product research and development
- Existing and future product designs and performance specifications
- Marketing plans or techniques
- Schematics
- Client lists
- Computer programs
- Processes

Also, be aware of how these categories have been identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source. When these conditions are met the information falls into the General Proprietary Business Information category of CUI.

DOES CUI INCLUDE PERSONALLY IDENTIFIABLE INFORMATION (PII) AND HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) REQUIREMENTS?

HIPAA Information, which includes all medical information, and PII have additional legal protection requirements that require consideration and may supersede CUI requirements. Industry is encouraged to work with their Contracting Officer Representative (COR) to understand requirements for handling each type of information.

WHAT POLICIES GOVERN CUI?

Four main policies govern CUI. Industry partners who currently have contracts with CUI requirements or anticipate such contracts in the future should familiarize themselves with all such policies.

1. Executive Order 13556 "Controlled Unclassified Information" This Instruction establishes policy,

assigns responsibilities, and prescribes procedures for CUI throughout the DOD and establishes

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. DoDI Instruction 5200.48 "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.

In some cases, DoDI 5200.48 includes more stringent requirements than the other policies. When this occurs, DOD Industry partners must follow the more stringent requirements.

IS CUI TRAINING AVAILABLE? IS IT MANDATORY?

The Center for Development and Security Excellence (CDSE) provides CUI training that is available to Industry. Per DoDI 5200.48 and pursuant to contractual requirements, DOD contractors require initial training and annual refresher training on CUI. Industry should note that this requirement is different from agencies governed by 32 CFR 2002, which requires refresher training every two years.

While CUI training is mandatory, Industry may choose to use the CDSE training or create its own training. When a contractor elects to create training, it MUST contain the 11 topics outlined in CUI Notice 2016-01.

HOW DOES CUI ALIGN WITH CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)?

Per CMMC Frequently Asked Questions, DOD is migrating to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). CMMC is intended to serve as a verification mechanism to ensure that DIB companies implement appropriate cybersecurity practices and processes to protect FCI and CUI within their unclassified networks. The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) manages the CMMC program.

WHO IS RESPONSIBLE FOR CONTROLLING CUI?

Anyone who creates information that is considered CUI is responsible for protecting and correctly handling it. Formally, 32 CFR Part 2002 designates the National Archives and Records Administration (NARA) as the program's Executive Agent (EA). NARA houses the Federal CUI Registry and is the overall point of contact for CUI-related regulations within the Executive Branch. DCSA is tasked with CUI Program Implementation for the DOD.

WHAT IS DCSA'S ROLE REGARDING THE CUI PROGRAM?

DoDI 5200.48 (March 2020) directs DCSA with eight responsibilities with respect to CUI:

- Administering the DOD CUI Program for contractually established CUI requirements for contractors in classified contracts.
- Assessing contractor compliance with NISP in accordance with 32 CFR 2003 and NIST SP 800-171.
- Establishing and maintaining a process to notify the DOD CIO, USD (R&E), and USD(A&S) of threats related to CUI for further dissemination to DOD Components and contractors.
- Providing security education, training, and awareness on the topics defined in 32 CFR 2002.30 to DOD personnel and contractors through the CDSE.
- Providing security assistance and guidance to the DOD Components on the protection of CUI when DOD Components establish CUI requirements

in DOD classified contracts for NISP contractors falling under DCSA security oversight.

- Serving as the DOD-lead to report Unauthorized Disclosure (UD) of CUI, except for the reporting of cyber incidents in accordance with Section 252.204-7012 of the Defense Federal Acquisition Regulation Supplement (DFARS), associated with contractually established CUI system requirements in DOD classified contracts for NISP contractors falling under DCSA oversight.
- Coordinating with the DOD Chief Information Officer (CIO) to implement uniform security requirements when the information systems or network security controls for unclassified and classified information are included in DOD classified contracts for NISP contractors falling under DCSA oversight.
- Consolidating DOD Component input on the oversight of CUI protection requirements in DOD classified contracts for NISP contractors under DCSA security oversight.

The Office of the Under Secretary of Defense for Intelligence and Security (OUSD (I&S)) is the DOD's Senior Agency Official for Security establishing policy and providing oversight of the DOD Information Security Program. As such, they coordinate with NARA, report on DOD's CUI status, and establish protocols for resolving disputes about implementing or interpreting CUI Program policies within and between DOD components. They also coordinate with both the DOD CIO and the CUI EA on CUI waiver requests and submit changes to CUI categories.

WHAT IS DOD'S TIMELINE FOR IMPLEMENTING CUI REQUIREMENTS?

CUI protection under E.O. 13556 has been in effect since December 2010, and each U.S. Government agency has begun to implement guidance to protect CUI and is required to implement their CUI Programs by the end of calendar year 2021. All active contracts should now have CUI requirements in place though in some cases the effort is ongoing. If Industry is uncertain of CUI requirements, they should consult with Government Contracting Activities for each effort in question.

IS DOD FOLLOWING THE SAME PROCESS AND TIMELINE FOR CUI AS ARE OTHER FEDERAL AGENCIES?

CUI is a government-wide directive mandated by Executive Order 13556. Agencies are implementing CUI on different schedules, and information provided by DCSA may not be applicable to other agencies. Industry partners are encouraged to work with their Government Contracting Activities to understand their specific CUI requirements and implementation timelines.

WHERE ARE CUI CATEGORIES LOCATED?

There are two useful CUI Registries for DOD contractors providing government-approved CUI Categories and Organizational Index Groupings.

- NARA ISOO National CUI Registry
- DOD CUI Registry

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.

HOW IS CUI MARKED?

At a minimum, CUI markings for unclassified DOD documents will include the acronym "CUI" in the banner and footer of the document. Portion markings may also be used but are not required. Marking requirements apply to documents, emails and forms of media that are designated as CUI. Furthermore, marking labels are available for media such as USB sticks, hard drives, and CD ROMs to alert holders to the presence of CUI stored on the device in accordance with CUI Notice 2019-01. The labels can be found in the DOD CUI Marking Guide.

The National Industrial Security System (NISS) is currently authorized to process and store CUI.

FAQs

WHO CAN CREATE CUI?

Anyone can create CUI as long as it is generated for, or on behalf of, an Executive Branch agency under a contract and it falls into one of the over one hundred DOD CUI categories. However, in most situations, Industry will be guided by its customer on what is CUI and what isn't.

WHAT ARE THE REQUIREMENTS FOR DISSEMINATING, DECONTROLLING, AND DESTROYING CUI?

Similar to other information requiring safeguarding, there are rules regarding dissemination, decontrol, and destruction of CUI. While the points below highlight these requirements, one should consult DoDI 5200.48 for a more comprehensive description.

- **Disseminate**. Authorized holders may disseminate CUI in accordance with distribution statements and applicable laws. Dissemination is allowed as long as it complies with law, regulation, or government-wide policy; furthers a lawful government purpose; is not restricted by Limited Dissemination Control (LDC); and is not otherwise prohibited by any other law, regulation, or government-wide policy.

  CUI information and material can be sent via first class mail, parcel post, or bulk shipments. CUI can also be transmitted by e-mail when practical, via approved secure communications systems, or systems using other protective measures.
- **Decontrol**. Once information is no longer CUI, it must be promptly decontrolled. Prior to decontrolling, the Director of the Washington Headquarters Services (WHS) will review CUI documents and materials for public release, in accordance with DoDI 5230.09. Once it is determined that the information no longer requires protection from public disclosure, the Federal Government will notify all known holders of the decontrolled information.
- **Destroy**. If there is no longer a use for CUI documents or materials, all hard and soft copies should be destroyed rendering it unreadable, indecipherable, and irrecoverable.

WHAT ARE LEGACY MATERIALS, AND DO THEY NEED TO BE REMARKED FOR CUI?

Sensitive types of unclassified information (such as information marked as FOUO or SBU) that was marked prior to the implementation of the CUI program which meets the standards for CUI is considered legacy information. Legacy documents do not need to be remarked until and unless the information is re-used, restated, or paraphrased. When new documents are derived from legacy documents, they must follow the new CUI marking standards.

For example, according to DoDI 5200.48, when citing legacy information in a new document, one must review the information for CUI and update the markings accordingly. However, it is important to note that legacy information does NOT need to be marked if it is not being disseminated outside of the DOD.

HOW WILL INDUSTRY KNOW ITS CONTRACTS REQUIRE CUI?

The federal entity requesting services shall determine CUI requirements for both unclassified and classified contracts. CUI shall be identified in the issuing DD254, Request for Quote (RFQ), Request for Proposal (RFP), and or supporting contract documentation when they exist. For existing contracted efforts, Industry should review current contracts and engage with Government Contracting Activity (GCA) to determine which, if any, CUI requirements are applicable to current contracts and the appropriate way forward.

Additionally, the FAR 52.204-2 and NISPOM 4-103 require a DD254 be issued by the government for each invitation for a bid, RFP, or RFQ requiring access to classified information.

WHAT RESPONSIBILITY DOES A PRIME CONTRACTOR HAVE TO ENSURE ITS SUBCONTRACTORS AND SUPPLIERS COMPLY WITH THE CUI PROGRAM?

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

WHAT CAN INDUSTRY DO TO PREPARE FOR CUI IF IT CURRENTLY HAS NO CONTRACTS THAT SPECIFICALLY REQUIRE IT?

Even if an Industry partner currently has no contracts with CUI requirements, they are encouraged to ensure they have an inventory of current legacy information. It is also important to understand that unclassified engagements with the DOD can also include FCI and CUI data that are not necessarily a part of a classified DOD contract. Industry should also ensure they understand CUI policies and requirements for future work. Additionally, contractors will likely have FCI and will be subject to CMMC requirements.

WHAT ARE THE REQUIREMENTS FOR SELF-INSPECTIONS REGARDING CUI FOR INDUSTRY?

DCSA is currently working on updating the Self-Inspection Handbook to include a section dedicated to CUI.

WHEN WILL DCSA BEGIN CONDUCTING CUI RELATED INSPECTIONS?

DCSA will not include CUI-related compliance in the scope of Security Reviews conducted in FY22. Industry is urged, however, to begin now to implement CUI safeguards if it has not already done so and ensure they are aware of CMMC requirements

HOW CAN INDUSTRY LEARN MORE ABOUT THE APPROVED SYSTEMS AND SERVICES AVAILABLE FOR HANDLING CUI MATERIALS?

Industry may reference the NIST SP 800-171 to learn more about the systems and services requirements for handling CUI.

Before selecting Cloud services, Industry should contact their GCA to request guidance on Cloud storage for CUI.

WHERE DOES INDUSTRY GO WITH QUESTIONS OR CONCERNS ABOUT HOW CUI IS BEING IMPLEMENTED FOR EXISTING CONTRACTS?

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

WHAT TOOLS AND TEMPLATES ARE AVAILABLE FOR INDUSTRY?

The DOD and other Federal agencies provide several resources and tools for industry and are working on more. The following websites provide helpful resources, CUI governing policies, and available training

- https://www.dcsa.mil/mc/ctp/cui
- https://www.dodcui.mil
- https://www.archives.gov/cui
- https://www.cdse.edu/catalog/elearning/IF141.html
- https://www.cdse.edu/toolkits/cui/current.html

CONTROLLED
UNCLASSIFIED
INFORMATION

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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