CYBERSHEATH

CUI Handbook

What You Need to Know About Controlled Unclassified Information

As you begin your journey to CMMC 2.0, DFARS 7012, or NIST 800-171 compliance, understanding how to identify and safeguard CUI becomes critical. This category of data demands protection pursuant to federal laws, regulations, and government-wide policies.

It can be a challenge to figure all this out on your own, and identifying and managing your CUI is a contractual requirement. Where do you start—and how do you proceed? The information provided here gets you started.

What is Controlled Unclassified Information (CUI)?

According to 42 CFR 2002.4, CUI is, "Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency."

CUI was established by Executive Order 13556 as a way to standardize how to handle sensitive but unclassified information. According to this order, "CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended."

Resources

- National Archives and Records Administration (NARA) CUI Registry: This is a registry of all CUI categories. It has links to the specific law, regulation, or government-wide policy that causes that category of information to be designated as CUI. https://www.archives.gov/cui/registry/category-list
- Department of Defense (DOD) CUI Registry: This registry highlights those categories that are in the NARA registry but are relevant to DOD contracts. Some of the NARA CUI categories

are relevant to other federal government agencies. It also provides links to additional resources. https://www.dodcui.mil/Home/DoD-CUI-Registry/

Examples of CUI

CUI is not a one-size-fits-all designation and can take many forms including:

- Controlled technical information (CTI), such as engineering drawings, technical reports and notes, bills of materials, software executables and source code
- Export controlled information (EAR or ITAR)
- For official use only (FOUO) documentation, which is under the DOD realm, but no longer a valid classification.
- Operations security (OPSEC) plans

This list is not exhaustive. Be sure to learn more about CUI to see where you have this type of data in your organization.

What is basic CUI and what is specified CUI?

Once you've identified your data as CUI, there is also another layer of designation to consider as all CUI is either CUI Basic or CUI Specified.

CUI Basic

CUI Basic is the subset of CUI for which the authorizing law, regulation, or government-wide policy does not have any specific handling or dissemination requirements. CUI Basic is handled according to the uniform set of controls set forth in the Code of Federal Regulations and the CUI Registry. This is sensitive information with no additional or different requirements mentioned in the underlying authorities. Most CUI will be Basic.

CUI Specified

CUI Specified is the subset of CUI in which the authorizing law, regulation, or government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. This is not a higher level of CUI, just a different level. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic. The distinction is that the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information.

Resources

- https://www.gsa.gov/system/files/508-GSA-CUI-Guide%201-31-2024.pdf
- https://www.archives.gov/cui/registry/cui-glossary.html

Identifying CUI

The first step in identifying CUI is to understand what CUI is and where it is present in your organization. Start by participating in the mandatory CUI training that the DOD (link down the page to that section) provides. Then begin going through each document your organization holds and determine if it contains CUI.

Once you understand the various information categories, you next need to map the information your company holds to the contracting regulations you must adhere to. Depending on your relationship with the DOD, there are a number of requirements to protect non-public information (NPI).

Information types include:

- **Federal Contract Information (FCI)** - Non-public information associated with a federal contract. CMMC offers this description, "FCI means information provided by or generated for the Government under a contract not intended for public release."
- **Covered Defense Information (CDI)** - A form of CUI that is developed under a DOD contract. It is non-public information where a specific law, regulation, or government-wide policy is published that requires that information to be protected in some manner.
- **CUI** - Established by Executive Order 13556 as a way to standardize how to handle sensitive but unclassified information. According to this order, "CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended."

As you work to identify the CUI you are handling, take the time to review your contracts and reach out to your contracting official to discuss the issue.

Categorizing and Marking CUI

After you identify your organization's CUI, it's time to set up labels to help you start shaping your dataset. These can include a nonsensitive information label, a CUI label, and further labels as

required if you need to have other categories. From a compliance perspective the labeling of your information gives you a clearcut definition of what CUI is and what it isn't. The hard part is that the government doesn't always inform your business what CUI is actually being generated on their end.

If you have difficulty determining the type of CUI that your organization has, it makes sense to visit the NARA website, which presents categories of CUI (https://www.archives.gov/cui/registry/category-list). This archive has all of the types of CUI and the markings that need to be used. There are many different categories.

Take the time to:

- Look at the NARA archive.
- See what is closest to what you need and make your own classification guide until the federal government gets mature in this process.
- When in doubt, mark the data you determine needs to be controlled as CUI.

Banner Marking	**CUI Category**	**Organization Grouping**
CUI//SP-CTI	Controlled Technical Information	Defense
CUI//SP-CEII	Critical Energy Infrastructure Information	Critical Infrastructure
CUI//SP-EXPT	Export Controlled	Export Control
CUI//SP-FISA(B)	Foreign Intelligence Surveillance Act (Business Records)	Intelligence
CUI//SP-PRVCY	Privacy	Privacy
CUI//SP-PROCURE	General Procurement & Acquisition	Procurement & Acquisition
CUI//SP-PROPIN	General Proprietary Business Information	Proprietary Business Information

Banner Marking	CUI Category	Organization Grouping
CUI//SP-CTI	Controlled Technical Information	Defense
CUI//SP-NNPI	Naval Nuclear Propulsion Information	Defense
CUI//SP-SRI	Nuclear Security Related Information	Nuclear
CUI//SP-PERS	Personnel Records	Privacy
CUI//SP-MFC	Proprietary Manufacturer	Proprietary Business Information
CUI//SP-PCII	Protected Critical Infrastructure Information	Critical Infrastructure
CUI//SP-DCNI	Unclassified Controlled Nuclear Information – Defense	Defense
CUI//SP-UCNI	Unclassified Controlled Nuclear Information – Energy	Nuclear

Resources

- CUI categories https://www.archives.gov/cui/registry/category-list
- CUI classification markings https://www.archives.gov/cui/registry/category-marking-list

Protecting CUI

You've identified and categorized your CUI, now it's time to make sure it's protected. Outline the boundaries of the system or network that houses CUI, define the areas where CUI is present, and identify who has access to it. Defining your CUI scope happens within the system security plan (SSP). That's where you outline your system boundaries.

Understand which assets are involved in storing, processing, or transmitting CUI, and then establish and document the security boundaries that segregate CUI from non-CUI assets. To do this, you need to find everywhere in your environment where CUI is flowing. You need to identify any

possible connection, whether that's internal or external, where you might be doing data transfers that may contain CUI. Some companies receive CUI data via removable media such as CDs, DVDs, or USBs. Others are sent physical items from government entities to their environment. It all depends on what your organization does. Keep in mind that CUI can include physical and digital assets.

Don’t take the path of most companies where they don't know what their CUI data set is, so they assume it's everything. Proceeding with this worst case scenario, means you assume that everyone has access to CUI and everyone needs access to CUI. Scoping how to protect this information becomes immense.

There's no one path for managing CUI.

That’s the bad news. The good news is there is an approach we apply to help uncover, define, and wrangle CUI. Once you scope your environment and understand how the data flows, you can then diagram your environment. It doesn't need to be technical, but it does need to outline where you are keeping the data, perhaps in Office 365 or in a locked room. You also need to document your processes around sending that data. Whether it's physical or digital data, you’ll need to follow certain processes. The goal is to have your CUI management documented in a policy and in a diagram as well as have some type of technical configuration to adhere to.

How did CUI get started, and why is it in contracts now?

In November 2010, President Barack Obama issued Executive Order 13556 "Controlled Unclassified Information" (the Order), establishing the Controlled Unclassified Information (CUI) program to standardize the handling of unclassified information requiring protection. Following that event and over the years, there were clauses, mandates, and requirements issued. Here’s a timeline showing the progression.

- October 2016: The DOD issued DFARS Clause 252.204-7012, requiring defense contractors to implement NIST SP 800-171 to protect CUI.
- December 2016: NIST SP 800-171 Rev. 1 is published, establishing the controls to implement to satisfy DFARS 252.204-7012.
- February 2020: NIST SP 800-171 Rev. 2 is published, and subsequently updated and reshared on 1/28/21.
- September 2020: DOD published an interim rule to the DFARS, establishing CMMC 1.0, 5-Level Model.
- November 2021: DOD announced CMMC 2.0, which broke CMMC down to 3-Level Model.

- May 2024: NIST SP 800-171 Rev. 3 Published. DOD provided a memo that Rev. 3 will not be required at this time.

DOD Mandatory CUI Training

CUI training is mandatory for industry when it is required by Government Contracting Activities for contracts with CUI requirements.

To learn more and access a course, visit these government sites.

- https://www.archives.gov/cui/training.html
- https://www.cdse.edu/Training/Controlled-Unclassified-Information-CUI-Training/
- https://www.dodcui.mil/Training/
- https://securityawareness.usalearning.gov/cui/index.html

CyberSheath offers a free annual six-session course to prepare you for CMMC 2.0, including learning all about CUI and how to protect this dataset. Learn more about this training program and be sure to sign up when it is next available.

CUI FAQs

How does CUI flow through an organization?

Here's an example of how CUI permeates an environment.

- Company A works with NASA and has rocket parts physically shipped to them. Their approved method for receiving those parts is through UPS.
- Those rocket parts then have a corresponding set of users who are allowed to receive them, bring them into the building, and document that they received them in accordance with the procedures they have in place.
- Company A also has another subsection of users who are going to work on those parts. Perhaps that includes engineers who draw plans, mechanical engineers who print or build parts, and management overseeing the work.
- All of these users are touching the CUI.

Other CUI examples

- If B Manufacturing is receiving technical data from a contract and they are the manufacturer who's producing the physical part, there are many layers to the CUI that need to be protected, including technical, physical, and digital data. At any point, the company can split the data up and have multiple departments involved, including accounting which is billing for the part.
- If C Construction is building a new government building, the plans for that structure are going to be CUI. Perhaps less obviously, most likely the location where it is being built is also CUI.

What are the asset categories involved in CMMC, including CUI?

- **CUI Assets** are directly involved in storing, processing, or transmitting CUI. These are known assets. This could be your endpoints, file shares, manufacturing equipment, or mobile devices.
- **Security Protection Assets** provide security functions to CUI assets. This is everything that you do to protect your environment, to safeguard CUI, and provide CUI flow control, including firewalls, intrusion protection, and intrusion detection.
- **Contractor Risk Managed Assets** are not intended to handle CUI but may do so due to their proximity or connectivity to CUI assets.
- **Specialized Assets** may or may not process, store, or transmit CUI. Assets include government property, internet of things (IoT) devices, operational technology (OT), restricted information systems, and test equipment,
- **Out-of-Scope Assets** are those that do not and cannot interact with CUI and must be physically or logically separated from CUI assets.

The top two items, CUI assets and security protection assets, for certain, according to the CMMC Level 2 scoping guidelines, would have to meet NIST 800-171 requirements. Contractor risk managed assets and specialized assets offer some flexibility in the requirements.

Navigating CUI Management: A Critical Responsibility

Understanding and managing CUI is a critical step in achieving compliance with CMMC 2.0, DFARS 7012, and NIST 800-171 requirements. By identifying, categorizing, and safeguarding your CUI, you can not only meet federal mandates but also protect your organization's reputation and competitiveness. While the process may seem overwhelming, leveraging resources like NARA, the DOD CUI Registry, and specialized training can simplify the journey. Remember, effective CUI management is not just about compliance—it's about building trust, securing contracts, and

safeguarding sensitive information critical to national security. Take the necessary steps today to ensure your organization is prepared for the challenges and opportunities ahead.

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