Do I Have CUI?

A Contractor's Field Guide

Many companies handling Controlled Unclassified Information (CUI) do so unaware of what they are actually handling. Yet, CUI is unclassified government information that still has to be protected. If your company has it, a contract clause requires you to protect it by implementing all 110 security requirements in NIST SP 800-171, and CMMC is how the Department of War checks that you did.

So the question "do I have CUI?" is the first question, not a detail to sort out later.

A NOTE ON CMMC TIMING

On 13 July 2026 the Department of War suspended the move to CMMC Phase 2, pausing the requirement for third-party (C3PAO) assessments. That pause did not change the standard. DFARS 252.204-7012, NIST SP 800-171R2, Phase 1 self-assessments, annual affirmations, DIBCAC assessment authority, and False Claims Act exposure all remain in effect. Identifying CUI correctly is no less urgent than it was in June.

Why this question decides everything else

DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" is the clause that creates the obligation to protect CUI. With this clause in your contract you are required to:

- Implement the 110 security requirements in NIST SP 800-171 on any system that stores, processes, or transmits that information
- Report a cyber incident to dibnet.dod.mil within 72 hours of discovering it

- Use cloud services that meet the FedRAMP Moderate baseline, or equivalent, for that information
- Flow the same clause down to any subcontractor you send the information to

The clause defines covered defense information as unclassified information described in the CUI Registry that is either **marked or otherwise identified in the contract**, or **collected, developed, received, transmitted, used, or stored by you in support of contract performance**.

STEP 1

Start with the contract, not the data

Before you look at a single file, open the contract. These clauses tell you what the government expects, and they are the first thing an assessor will ask to see.

LOOK FOR	WHAT IT MEANS
DFARS 252.204-7012	You are expected to handle covered defense information. The 800-171 obligation attaches.
DFARS 252.240-7997 Older contracts: 252.204-7019 / 7020	You must give DoD access to your facilities and systems for a government-run Medium or High assessment. The old standalone requirement to post a basic self-assessment score in SPRS was dropped on February 1, 2026; your SPRS entry now comes through CMMC.
DFARS 252.204-7021	A CMMC status is a condition of award and must be maintained through performance.
DFARS 252.204-7025	The solicitation is telling you which CMMC level and assessment type this contract requires.
FAR 52.240-93 Older contracts: 52.204-21	Basic safeguarding of federal contract information. This is the floor, and it applies even with no CUI.
Distribution statements B through F on drawings, specs, or SOWs	The technical data is export-controlled or otherwise restricted. Strong signal of Controlled Technical Information.

Two things people miss

Flow-downs count.

If you are a subcontractor, the prime is required to pass 252.204-7012 down to you. Your obligation comes from your subcontract, not from a direct relationship with the government. Check the subcontract terms, the purchase order, and any supplier quality clauses attached by reference.

The clause can be present when the CUI is not, and the reverse.

A clause in your contract is not by itself proof you hold CUI, and a contract silent on CUI does not mean the drawing in your email is safe to forward. The clause tells you what the obligation is. The next two steps tell you whether it has been triggered.

STEP 2

Read the markings

When CUI is marked correctly, the marking tells you three things: that it is CUI, what kind, and who to call.

The banner

The word CUI in bold capitals, centered at the top and bottom of every page. That is the minimum. A fuller banner adds the category and any dissemination limits, separated by double slashes:

```
CUI
CUI//SP-CTI
CUI//SP-CTI//NOFORN
```

Portion markings

Parentheses at the start of each paragraph, section, or slide showing what that specific portion is. (CUI) for a controlled portion, (U) — short for Unclassified — for a portion that is not CUI and needs no protection. Not every document is portion-marked, but when it is, you can tell exactly which paragraph carries the sensitivity.

```
CONTROLLED UNCLASSIFIED INFORMATION

MEMORANDUM FOR RECORD

SUBJECT: (U) Delivery Schedule, Contract W911QY-26-C-0042

1. (U) This memorandum confirms the schedule agreed at the
   30 September program review.

2. (CUI) Bracket assembly P/N 7741-203 shall be heat-treated to
   the profile at Appendix B. That profile was developed under
   government specification and is not releasable to the public.

3. (U) Direct questions to the contracting officer.

Controlled by: Program Office, XYZ Manufacturing
CUI Category: CTI (Controlled Technical Information)
Distribution Control: FEDCON
POC: J. Alvarez, 555-0142

CONTROLLED UNCLASSIFIED INFORMATION
```

The designation indicator

A small block in the lower-right corner or footer of the first page. It carries four things:

```
Controlled by: [Organization]
Controlled by: [Office]
CUI Category: [e.g. SP-CTI]
Distribution/Limited Dissemination Control: [e.g. NOFORN]
POC: [phone or email]
```

That POC line is the single most useful item on the page. It is the person who can answer your question about this document, and it is a best practice rather than a requirement, so it is often missing.

Dissemination controls

Dissemination controls tell you who may see it.

- **NOFORN** means no foreign nationals, including your own employees who are not U.S. persons.
- **REL TO USA, [country]** permits named partners.
- **DL** points to a named dissemination list.

These controls are about people, not just systems, and they are where small companies get caught: an export-controlled drawing sitting on a shared drive that a non-U.S.-person engineer can open is a problem no firewall solves.

The control rides in the banner after a double slash, and the same words repeat in the designation block at the end. These are the ones you are most likely to see:

`CUI//SP-CTI//NOFORN`	No foreign nationals may see it. Applies to your own employees who are not U.S. persons, not only to people outside the company.
`CUI//SP-CTI//REL TO USA, GBR, AUS`	Releasable to the named countries only. Anyone else, including other allies, is still excluded.
`CUI//SP-PRVCY//FEDCON`	Federal employees and contractors only. Rules out a state agency, a university partner, or a trade group.
`CUI//SP-CTI//FED ONLY`	Federal employees only. Contractors are excluded, which can include you.
`CUI//SP-EXPT//DL ONLY`	Only the people on a named distribution list that the originator maintains. If you are not on it, ask before forwarding to anyone.

Two practical notes. These controls are set by the agency that created the document, so you cannot add or drop one on your own — if a control is in your way, the fix is a conversation with the contracting officer, not a redesigned marking. And a control that limits people does not relax when the document moves to a system. NOFORN on a file in a compliant cloud environment still means the non-U.S.-person engineer with a valid account may not open it.

The federal government establishes the legal authorities and approved categories under which information qualifies as CUI. **Contractors cannot independently create new CUI categories or designate arbitrary information as CUI.** However, when authorized through a government contract or supporting documentation, contractors may identify, designate, and mark information as CUI, including newly generated information that independently meets an established CUI category. Contractors must also preserve appropriate CUI protections and markings when incorporating previously designated CUI into new documents.

STEP 3

What if it isn't marked?

This is a situation that often happens. A drawing arrives by email from your prime. It looks sensitive. Nothing on it says CUI. Your contract has 252.204-7012 in it. What now?

The wrong instinct is to conclude it is not CUI because nobody marked it. Marking is the designating agency's job, and agencies and primes miss it constantly. The absence of a marking tells you about their process, not about the data.

The equally wrong instinct is to treat everything as CUI. That sounds safe but becomes expensive because it drags systems, people, and vendors into your assessment boundary that never needed to be there, and it makes your scope impossible to defend to an assessor who asks why.

The workable answer is in between: protect it as if it were CUI while you get an answer in writing. Here are the steps you should follow:

1. **Contain it now.** Move it out of general email and shared drives into whatever controlled environment you have. Do not forward it.
2. **Ask the source, in writing.** The prime's contracts or program contact, or the government contracting officer named in your contract. Email, not a phone call. You want the answer on paper.
3. **Ask a specific question.** Not "is this sensitive?" but the three questions in Appendix B.
4. **File the answer.** Keep the reply with your System Security Plan. When an assessor asks how you decided what is in scope, this correspondence is the evidence.
5. **If no answer comes,** keep protecting it, document that you asked and when, and escalate through your contracts channel. A documented unanswered request is a defensible position. Silence plus an unprotected file is not.

The clause also covers information you develop in performance of the contract, not only what the government sends you. A test report, a process sheet, or a quote to a sub that embeds controlled dimensions: if it derives from CUI, it is CUI, and nobody is going to mark it for you.

NEXT

The answer is yes. Now what?

Two things happen next, and only one of them is technical.

1. First, draw the boundary

Decide where CUI is allowed to live, and then work to secure that environment. Every system, service, and person that stores, processes, or transmits CUI is in scope for your assessment. Every one you keep it out of is not. **This is the single largest cost lever you control.** A company that lets CUI sit in ordinary email and file shares has just put its entire IT estate in scope. A company that confines CUI to one controlled environment has a scope it can afford to secure and can explain to an assessor in a sentence.

2. Second, handle it correctly day to day

At rest. Use encrypted storage inside the boundary - not personal drives, not consumer file sharing, not a laptop nobody manages.

In transit. Data in transit must also be encrypted. Ordinary email is not a CUI channel. This is the most common failure in the defense industrial base, and it is the one that puts the data in a prime's inbox, a personal account, and a mail server you do not control, all at once.

Access. Only people who need it for the contract should be able to access it, and only U.S. persons where a dissemination control or export restriction says so. This includes your IT provider and anyone with administrative access to the environment.

Marking. Carry the CUI designation forward onto anything you derive from it.

Destruction. Shred paper to the required standard and sanitize media. Deleting a file is not destroying it.

Incidents. If CUI is compromised, you have 72 hours to report at dc3.mil. Know now who makes that call, because 72 hours is not long enough to work it out later.

Subcontractors. Flow the clause down, and know which of your suppliers receive CUI. Their exposure is your exposure.

Five mistakes that cost points

1. **"Nobody marked it, so it isn't CUI."** Unmarked CUI is still CUI. The designation comes from the contract and the source, not from a stamp someone forgot.

2. **"We only protect what the government sent us."** The clause covers what you develop, receive, use, and store in performance of the contract. Your own output counts.

3. **Treating everything as CUI.** Over-scoping is not the safe choice. It inflates cost and it produces a boundary you cannot justify when an assessor asks why a given system is inside it.

4. **Leaving CUI in ordinary email.** It is the most common path by which a controlled drawing ends up on an unmanaged mail server, a personal phone, and a supplier's inbox. Email is where scope quietly expands.

5. **Making the determination verbally.** You will be asked how you decided. "We talked to the prime" is not evidence. The email is.

WORKSHEET

Take this to your Monday meeting

Seven questions. If you cannot answer one of them, that is where your work starts.

1	Which of our contracts contain DFARS 252.204-7012? Who can produce that list today?
2	Which contracts came to us as flow-downs from a prime, and have we read those terms?
3	What information do we receive, and what do we create, that is CUI? Name the actual documents.
4	Where does that information live right now: every system, every drive, every mailbox, every supplier?
5	Who has access to it, and are any of them not U.S. persons where a restriction applies?
6	Who sends the determination email when something arrives unmarked, and where do we file the answer?
7	Who reports a cyber incident within 72 hours, and do they know that is their job?

The useful outcome of this meeting is not a decision. It is a named owner and a date for each line above.

Where PreVeil fits

Once you know what your CUI is, the boundary decision above determines much of your cost. PreVeil helps you protect that boundary.

PreVeil is end-to-end encrypted email and file sharing built for CUI. It creates a secure, controlled environment alongside the systems you already use, so CUI moves into PreVeil and stays out of ordinary email and file shares.

Over 100 customers have used PreVeil to reach a perfect 110 SPRS score and to pass DIBCAC and C3PAO assessments.

Come find us at the PreVeil booth, or start at preveil.com.

Prepared for CMMC Day 2026. This guide is educational and is not legal advice. Your contracting officer is the authority on what your specific contract requires.

APPENDIX A

What CUI actually looks like in a defense supply chain

The CUI Registry lists roughly 125 categories across 20 groupings. Most of them will never touch your business. They cover things like death records, campaign funds, and water assessments. Browsing the whole registry is how people talk themselves into confusion.

For a defense contractor or manufacturer, a small number of categories account for nearly everything:

CATEGORY	GROUPING	WHAT IT LOOKS LIKE ON YOUR NETWORK
Controlled Technical Information (CTI)	Defense	Drawings, specifications, process sheets, test data, engineering models, source code with military application
Export Controlled	Export Control	Anything subject to ITAR or EAR. Overlaps heavily with CTI on the same drawing.
General Privacy / Personnel Records	Privacy	Personnel data you hold because of a contract, not your ordinary HR file
Naval Nuclear Propulsion Information	Defense	Narrow, but absolute. If you touch it, you already know.
DoD Critical Infrastructure Security Information	Defense	Facility, security, or system data on protected infrastructure

If you make parts to a government drawing, Controlled Technical Information is your answer most of the time. Start there and work outward, rather than starting from the registry and working in.

APPENDIX B

The determination request email

Send this when something arrives unmarked and you need the answer on paper. Keep the reply with your System Security Plan.

Subject: CUI determination request — [contract or PO number]

Hello [name],

We received [document name / file] on [date] in connection with [contract or PO number]. The document is not marked, and we want to handle it correctly.

Could you confirm:

1. Is this document Controlled Unclassified Information?
2. If so, what CUI category applies, and are there any limited dissemination controls such as NOFORN?
3. If it is CUI, can you please provide a properly marked copy for our records?

Until we hear back, we are handling it as CUI.

Thank you,
[name]