

# ARE YOU HANDLING SENSITIVE DOD DATA WITHOUT REALIZING IT?

# **QUICK CHECKLIST Does This Sound Like Your Business?**

Use this simplified guide to help identify whether your organization is likely handling **CUI** or **FCI** (Federal Contract Information).



Check your DoD-related contracts or subcontract agreements. Do they include:



- 252.204-7012 (Safeguarding Covered Defense Information)
- 7019 or 7020 (CMMC requirements)
- Terms like CUI, CDI (Covered Defense Information), or CTI (Controlled Technical Information)?
- Flow-down requirements from a prime contractor that mention NIST 800-171 or CMMC?



If so, you're likely being asked to protect CUI—even if it's not spelled out clearly.



### TYPES OF DATA YOU RECEIVE OR CREATE

Do you work with:

- Engineering drawings, technical specs, or CAD files?
- Firmware, software source code, or testing procedures?
- Files labeled CUI, FOUO (For Official Use Only), or similar?
- Export-controlled data under ITAR or EAR?
- Defense-related systems, logistics, support, or maintenance?



Even if no one has said "you handle CUI," the type of data you touch may qualify.

If your company supports defense contracts—even as a subcontractor, supplier, or service provider—you may be working with sensitive government data protected under strict cybersecurity rules.

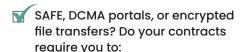
That data is called **Controlled Unclassified Information (CUI)**. If you receive, process, or store CUI, you're required to follow the **NIST SP 800-171** security framework. Soon, you may also need a **CMMC Level 2 certification** to keep bidding on or working under defense contracts.

But how do you know if this applies to you?



## SYSTEMS AND TOOLS YOU USE

Are you required to use secure DoD platforms, like:



- Encrypt data during transmission or storage?
- Protect systems that process sensitive defense-related info?



These requirements are strong indicators that you're working with CUI.

#### FCI VS. CUI: WHAT'S THE DIFFERENCE?

You might be handling both—even without realizing it.

| ТҮРЕ                                  | APPLIES WHEN YOU   | COMPLIANCE REQUIRED                      |
|---------------------------------------|--|--|
| FCI (Federal Contract Info)           | Work on most federal contracts                               | 15 basic controls<br>(FAR 52.204-21)     |
| CUI (Controlled<br>Unclassified Info) | Handle sensitive defense data<br>(e.g., drawings, ITAR data) | 110 controls<br>(NIST SP 800-171 + CMMC) |

FCI is the baseline. CUI comes with stricter requirements—and often more consequences.

#### YOU MAY BE HANDLING CUI IF YOU WORK WITH:

- Export-controlled designs or specs (ITAR/EAR)
- Proprietary or technical data from DoD
- Law enforcement-sensitive or privacy-related data (PII, PHI)
- Testing protocols or QA results for government systems

Still unsure? Check the CUI Registry at archives.gov/cui.

#### WHAT THIS MEANS FOR YOUR BUSINESS

If any checklist items apply, you likely have a responsibility to comply with NIST SP 800-171. Soon, you may also need to pass a CMMC Level 2 audit.

#### Failure to comply could lead to:

- Lost contracts
- Legal issues under DFARS or the False Claims Act
- Increased risk of cyber incidents

#### The good news?

You don't have to figure it out alone. With the right partner, you can:

- Identify what types of data you handle
- Understand your regulatory requirements
- Implement the right-sized security and compliance plan



#### **NOT SURE WHERE TO START?**

Here's what to do:



**Review your contracts** for DFARS clauses or flow-down requirements



**Evaluate your data:** Do you handle engineering specs, export-controlled info, or labeled files?



Assess your tools: Are you using DoD SAFE, encrypted email, or compliance-driven platforms?

Still unclear? We can help you figure it out.

#### WHY WORK WITH ISI?

We're not consultants who disappear after a gap assessment. We're not generalist MSPs who miss key compliance requirements. We're a purpose-built MSP for DIB-focused SMBs.

With ISI, you get:

- Integrated cybersecurity, IT, and compliance support
- Right-sized access to expert teams and proven tools
- Continuous monitoring and audit readiness

We help you protect your data, contracts, and reputation—so you can focus on growing your business.