🛡️ What Level of CMMC Certification Does My Business Require?

Created by EmTech Enterprises | Registered Compliance Support

🎯 Purpose of This Guide

This guide helps small and medium-sized businesses (SMBs) determine which level of Cybersecurity Maturity Model Certification (CMMC) they need based on the type of federal data they handle and their role in the defense supply chain.

🔍 Understanding the CMMC Levels

Level	Description	Who Needs It
Level 1: Foundational	Basic safeguarding of **Federal Contract Information (FCI)**	Most commercial contractors and subcontractors
Level 2: Advanced	Protection of **Controlled Unclassified Information (CUI)**	Contractors handling sensitive technical data
Level 3: Expert	Protection against **Advanced Persistent Threats (APTs)**	Prime contractors on high-priority DoD programs

🧠 Key Questions to Ask

1. **Do you receive or generate FCI?** → You likely need **Level 1**
   What is FCI?
2. **Do you store, process, or transmit CUI?** → You likely need **Level 2**
   What is CUI?
3. **Are you working on critical national security contracts?** → You may need **Level 3**, assessed by the DoD

🧩 How EmTech CyberShield™ Helps

- RP-led scoping to identify FCI and CUI boundaries
- SAT mapping to CMMC AT controls
- SSP and POA&M templates for audit prep
- Incident playbooks and escalation guides
- jAIme AI agent for real-time client support

🧬 Bonus: Role-Based Examples

Role	Likely CMMC Level
Commercial subcontractor with no CUI	Level 1
Manufacturer handling DoD drawings	Level 2
Prime contractor on missile systems	Level 3

📞 Ready to Find Your Level?

Schedule a free consultation with EmTech's RP team: 1-877-598-8736

Visit https://cybershield.emtechenterprises.com to get started.

What is FCI?

FCI stands for **Federal Contract Information**. It refers to information provided by or generated for the U.S. government under a contract that **is not intended for public release**.

🔍 What Counts as FCI?

- Contract details (e.g., schedules, pricing, deliverables)
- Internal communications related to federal work
- Non-public technical or operational data shared by the government

🧩 Why It Matters for CMMC

If your company handles FCI, you're required to meet **CMMC Level 1** — which includes 17 basic safeguarding practices based on FAR 52.204-21. These are foundational cybersecurity controls like:

- Limiting system access
- Updating antivirus software
- Training employees on security awareness

What is CUI?

CUI stands for **Controlled Unclassified Information**. It refers to sensitive federal data that **isn't classified but still requires safeguarding** under laws, regulations, or government-wide policies.

🔍 What Counts as CUI?

- Technical drawings, schematics, or blueprints from the DoD
- Export-controlled data (e.g., ITAR/EAR)
- Legal documents, financial records, or proprietary research tied to federal contracts
- Any information marked or designated as CUI by the government

🧩 Why It Matters for CMMC

If your business handles CUI, you're required to meet **CMMC Level 2** — which includes implementing all 110 practices from NIST SP 800-171. These controls cover:

- Access control and authentication
- Incident response and audit logging
- Secure configuration and media protection

FCI vs CUI: What's the Difference?

Feature	FCI (Federal Contract Information)	CUI (Controlled Unclassified Information)
Definition	Information provided by or generated for the government under contract, not intended for public release	Sensitive information that requires safeguarding under laws, regulations, or policies
Examples	Contract numbers, delivery schedules, internal communications	Technical drawings, DoD schematics, ITAR data, proprietary research
Marking	Not typically marked	Often marked as "CUI" or with category indicators
CMMC Level Required	Level 1 (Foundational – 17 practices)	Level 2 (Advanced – 110 practices from NIST SP 800-171)
Safeguards Needed	Basic cyber hygiene (e.g., access control, antivirus, training)	Full suite of security controls (e.g., audit logs, incident response, encryption)
Who Handles It	Most DoD contractors and subcontractors	Contractors working with sensitive defense-related data

Why This Matters

Knowing whether you handle FCI or CUI determines your required CMMC level, the controls you must implement, and the support you need from an RP or RPA.

How EmTech CyberShield™ Helps

- Identify and classify your data (FCI vs CUI)
- Map your environment to the right CMMC level
- Provide RP-led guidance, Control alignment, and technical safeguards
- Prepare your SSP, POA&M, and audit evidence