CMMC Guide Overview

CTS COMPANIES

Introduction

The defense industrial base (DIB) — consisting of over 300,000 companies supporting the United States Department of Defense (DoD) in research, development, acquisition, production, sustainment and services — is a particular risk for cybersecurity threats. To address these risks, the DoD **developed the CMMC framework** (*reference: U.S. Department of Defense CIO*).

Important Definitions:

- **Federal Contract Information (FCI):** Information provided by or generated for the government under contract, not intended for public release.
- **Controlled Unclassified Information (CUI):** Unclassified information that requires safeguarding or dissemination controls under laws, regulations, or policies; excludes classified national security information.

Purpose of This Document

This document presents the structure of CMMC — the "model" — including its levels, domains, and practices. It is meant to provide a common reference for DoD and DIB contractors when assessing cybersecurity maturity. It is not a conclusive representation of all requirements.

CMMC Model Overview

The CMMC framework builds on the following regulatory and standards sources:

- The basic safeguarding requirements for FCI under Federal Acquisition Regulation (FAR) clause 52.204-21.
- The security requirements for CUI defined in NIST SP 800-171 Rev 2, per Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.
- A subset of the enhanced requirements from NIST SP 800-172.

These requirements are organized into "domains" (control-families), and mapped into three maturity levels.

CMMC Certification Levels

Level	Purpose / Scope	Key Focus
Level 1	Protection of FCI (*not* CUI)	Implements the 15 basic safeguarding requirements from FAR 52.204-21.
Level 2	Protection of CUI	Implements the 110 security requirements from NIST SP 800-171 Rev 2.
Level 3	"Expert" level	Will implement a subset of enhanced requirements from NIST SP 800-172.

Cumulative Requirement:

you can only be certified to highest level that you are completely compliant. If you handle CUI, you MUST be certified to Level 2. If you have questions on the level to which you must certify, contact us at 248.334.5800 or info@cts-companies.com.

CMMC Domains (Control Families)

CMMC defines **14 domains**, aligning with the families in NIST SP 800-171.

Abbrev.	Domain Name	Abbrev.	Domain Name
AC	Access Control	**RA**	Risk Assessment
AT	Awareness & Training	**CA**	Security Assessment
AU	Audit & Accountability	**SC**	System & Commun. Protection
CM	Configuration Management	**SI**	System & Information Integrity
IA	Identification & Authentication	**PS**	Personnel Security
IR	Incident Response	**PE**	Physical Protection
MA	Maintenance	**MP**	Media Protection

These domains cover a broad spectrum of cybersecurity controls — from access restrictions and authentication to incident response, media handling, and system integrity.

Sample Practices by Domain & Level

Here are a few examples of practices under the CMMC model:

Access Control (AC)

- *Level 1 — Authorized Access Control:* Limit system access to authorized users, processes, or devices.
- *Level 2 — Least Privilege:* Ensure privileged and non-privileged accounts have only the permissions needed for their roles.
- *Level 2 — Control CUI Flow:* Ensure Controlled Unclassified Information is accessed and transferred only according to approved authorizations.

Identification & Authentication (IA)

- *Level 1 — Identification & Authentication:* Verify identity of users, processes, or devices before granting access.
- *Level 2 — Multifactor Authentication (MFA):* Require MFA for local and network access to privileged accounts, and network access to non-privileged accounts.

Incident Response (IR)

- *Level 2 — Incident Handling:* Establish procedures for detecting, analyzing, containing, and recovering from cybersecurity incidents.
- *Level 2 — Incident Reporting:* Log and report security incidents to designated personnel or authorities.

Media Protection (MP)

- *Level 1 — Media Disposal:* Sanitize or destroy media containing FCI before disposal or reuse.
- *Level 2 — Media Protection:* Securely store and restrict access to media containing CUI (digital or physical).

NOTE: the model includes dozens of additional practices across domains for Level 2, and more expected for Level 3.

Why CMMC Matters?

Supply-chain security:

Many DoD contractors depend on subcontractors and suppliers. CMMC aims to ensure that protection of FCI or CUI extends down the entire supply chain — not just the prime contractors' networks.

Assurance and accountability:

By certifying that companies have implemented defined cybersecurity practices, DoD can trust that sensitive information is handled securely.

Scalability for different risk levels:

With three levels, the model supports small contractors handling FCI only, as well as organizations managing sensitive CUI requiring stricter controls.

Alignment with existing standards:

The framework draws on established cybersecurity standards (FAR safeguarding + NIST SP 800-171 / 800-172), offering familiarity and a clear path for compliance.

Summary

The CMMC 2.0 Model provides a structured, tiered approach to cybersecurity for DoD contractors. It balances **baseline cybersecurity hygiene** for low-risk operations with **robust protections** for CUI, while offering a clear compliance path. For any organization working with the DoD — whether handling just FCI or also CUI — understanding and implementing the applicable CMMC level is critical to meet regulatory requirements and protect sensitive information.