CMMC Level 3 - Expert

Level 3 builds on Level 2 by adding enhanced protections for the most sensitive programs.

- Requires all 110 NIST SP 800-171r2 controls, plus an additional 24 controls from NIST SP 800-172
- Triennial government-led assessment
- Reserved for contracts supporting the highest national security priorities

CMMC GRADING

CMMC grading evaluates how effectively an organization has implemented required cybersecurity controls. Assessments focus on real-world implementation and operational maturity—not just written policies—and use a point-based methodology to measure completeness. Points are weighted based on risk, reinforcing the importance of strong cybersecurity fundamentals across the organization.

Organizations must successfully meet the assessment requirements for the applicable CMMC level in order to demonstrate compliance and be eligible for contract award.

WE CAN HELP

TotalCare IT helps Defense Industrial Base organizations prepare for CMMC by focusing on infrastructure readiness—the technical foundation required to support compliance.

- Secure configuration of workstations, servers, and network infrastructure
- Design and management of on-prem and cloud environments
- Implementation of technical controls and management of cybersecurity tools
- Aligning IT systems to support NIST SP 800-171 Revision 2 requirements

For formal compliance activities, TotalCare IT partners with trusted local cybersecurity firms and Certified Third-Party Assessor Organizations (C3PAOs). This collaborative approach ensures your organization is technically prepared before entering formal assessments. CMMC readiness does not happen overnight. Building a secure, compliant infrastructure early reduces risk, cost, and disruption later. Give us a call today to get started!

TotalCare IT
(208) 881-9713
www.TotalCareIT.net/cmmc

CMMC 2.0
Edition

THE POCKET GUIDE TO CMMC

for Defense Industrial Base Companies and Their Subcontractors

TotalCare IT
We Keep People Working

WHAT IS CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a Department of Defense (DoD) program designed to ensure that contractors and subcontractors across the Defense Industrial Base (DIB) adequately protect Federal Contract Information **(FCI)** and Controlled Unclassified Information **(CUI)**.

CMMC is designed to give the DoD a way to enforce the protection of national security information and American ingenuity.

CMMC only applies to **DIB** organizations—companies that support the research, development, production, or sustainment of military systems, subsystems, and components under contract with the DoD.

With the release of the CMMC 2.0 Final Rule in 2025, the DoD formally streamlined the program to reduce complexity while maintaining strong cybersecurity standards. CMMC is now closely aligned with NIST SP 800-171 Revision 2 and, at the highest level, NIST SP 800-172. *Note: NIST has released SP 800-171 Revision 3, but it has not yet been adopted by the DoD for CMMC purposes.*

CMMC has 3 levels of maturity, with each increasing in robustness of cybersecurity requirements, assessment rigor, and oversight. The required CMMC level will be clearly stated in solicitations and RFIs, and contractors are required to meet the specified level *before* contract award.

CMMC Level 1 - Foundational

Level 1 focuses on basic cyber hygiene and applies to organizations that handle FCI but do not process, store, or transmit CUI.

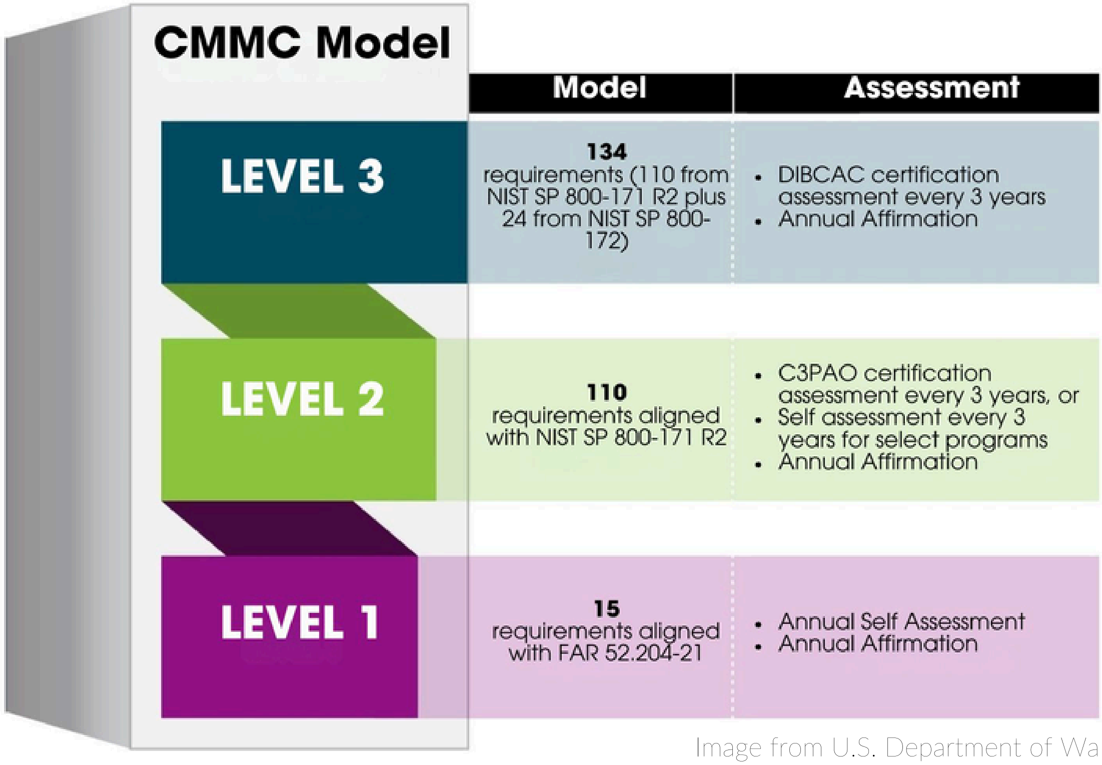
- Requires implementation of 17 practices aligned with FAR 52.204-21
- Annual self-assessment required
- Senior company official must affirm compliance

CMMC Level 2 - Advanced

Level 2 is designed for organizations that process, store, or transmit CUI.

- Requires full implementation of all 110 controls in NIST SP 800-171 revision 2
- Two assessment paths:
  - Annual self-assessment for select contracts
  - Triennial third-party assessment by a Certified Third-Party Assessor Organization (C3PAO) for contracts involving information critical to national security
- Scores are submitted to the Supplier Performance Risk System (SPRS)

Most DIB companies will fall into CMMC Level 2.



CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	• DIBCAC certification assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 R2	• C3PAO certification assessment every 3 years, or • Self assessment every 3 years for select programs • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual Self Assessment • Annual Affirmation

Image from U.S. Department of War