carahsoft.
TECHNOLOGY BY POLICY

CMMC

Cybersecurity Maturity Model Certification

December 26, 2023

Overview

Cybersecurity Maturity Model Certification (CMMC) is a DoD-wide program that provides a comprehensive framework to protect the Defense Industrial Base's (DIB) sensitive unclassified information from frequent and increasingly complex cyberattacks. CMMC was designed to increase the overall cybersecurity posture of the DOD supply chain by working on a tiered model with cumulative practices that build at each successive level. Assessment requirements include self-assessment, third-party assessments, and government assessments.

The Defense Federal Acquisition Regulation Supplement (DFARS) establishes the contractual foundation for enforcing CMMC requirements across the Defense Industrial Base (DIB). Together, **DFARS 7012, 7019, 7020, and 7021** mandate the protection of Controlled Unclassified Information (CUI), requiring contractors and subcontractors to implement **NIST SP 800-171 controls** and allowing the **DoD to verify compliance**.

Framework

The CMMC framework focuses on protecting CUI and Federal Contract Information (FCI) stored or processed on contractor systems. Security controls organized into **14 capability domains**, which include: Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communication Protection, and System and Information Integrity.

CMMC Model	Model	Assessment
Level 1	**15** requirements aligned with FAR 52.204-21	• Annual Self Assessment • 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 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

What Does This Mean for Government?

The Department of Defense will face new mandates to:

- Integrate CMMC certification requirements into all relevant solicitations, contracts, and task orders.
- Verify contractor compliance through approved third-party or government-led assessments before contract award.
- Align procurement processes to risk-based CMMC levels tied to the sensitivity CUI and FCI.
- Enforce timely remediation of cybersecurity gaps and maintain oversight through authorized audit and reporting systems such as SPRS and eMASS.

The CMMC framework represents a major advancement in DoD acquisition policy, establishing **cybersecurity as a mandatory prerequisite** for conducting business with the U.S. Government.

What Does This Mean for Industry?

For contractors, integrators, and vendors selling to the DIB, the CMMC framework requires them to:

- Implement CMMC-aligned security controls across networks, applications, and data storage environments.
- Map internal cybersecurity practices to the appropriate CMMC level based on contract requirements.
- Maintain auditable records and readiness for third-party or government-led assessments.
- Integrate continuous monitoring and risk management to mitigate evolving threats.
- Treat CMMC compliance not only as a regulatory requirement, but as a strategic differentiator in competing for DoD contracts.

CMMC compliance further requires coordination with accredited entities within the assessment ecosystem, including **Certified Third-Party Assessment Organizations (C3PAOs)**, **Assessors**, and the **CMMC Accreditation Body (AB)**. These entities ensure that all contractors, vendors, and service providers adhere to the rigorous security standards necessary to safeguard CUI across DoD environment.

Timeline

The first phase of CMMC implementation begins on **November 10, 2025**, launching a **four-phase rollout** over three years. Each phase incrementally adds CMMC requirements, starting with self-assessment and concluding with **full certification and enforcement**, allowing time for assessor training and industry readiness.

Phase	Key Dates	Implementation
Phase 1 - Initial Implementation	**November 10, 2025**	• Where applicable, solicitations will require Level 1 or 2 self-assessment
Phase 2	**November 10, 2026**	• Where applicable, solicitations will require Level 2 Certification • The Department may opt to delay the Level 2 Certification requirement in a contract to an option period
Phase 3	**November 10, 2027**	• Where applicable, solicitations will require Level 3 Certification • The Department may opt to delay the Level 3 certification requirement in a contract to an option period
Phase 4 -Full Implementation	**November 10, 2028**	• All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.