

Prepare for CMMC Certifications with Kratos Consulting Services



FCI and CUI

With many organizations preparing for the Cybersecurity Maturity Model Certification (CMMC) requirements, now is the time to prepare. It is anticipated that CMMC will be phased into DoD contracts starting in 2025 or early 2026. Once DoD begins phasing CMMC into RFPs, prime and subcontractors doing business with the DoD must achieve the required CMMC Status as a prerequisite to new contract awards.

The Cyber AB is continuing to authorize CMMC Third Party Assessment Organizations (C3PAO) while also vetting Registered Provider Organizations (RPO). Leveraging C3PAO and RPO subject matter experts best prepares your organization for an eventual assessment against CMMC practice requirements. Kratos provides several advisory services that accelerate time to certification.



Boundary Identification and Definition Support

- Analysis of the system environment to identify and define the authorization boundary
- Development of authorization boundary and data flow diagrams, along with a system inventory in accordance with the authorization boundary



Gap Analysis

- Simulates a C3PAO assessment, determining compliance against the CMMC practice requirements
- Includes recommendations for practice remediation and overall cybersecurity posture improvement
- Recommendations and priorities are condensed into a roadmap to drive efficient use of resources



Documentation Support Services

- Identifies gaps between existing documentation and CMMC practice requirements
- Supports the development of documentation that addresses all CMMC practice requirements
- Highlights how documentation meets objective evidence requirements
- Policy, procedure, and plan templates mapped directly to CMMC requirements available, as needed



Process and Engineering Consulting Services

- Provides requirements-driven recommendations on new existing processes and operations to ensure alignment with CMMC practice requirements
- Provides technical recommendations on architecture, configuration, tooling, reporting, and automation to meet CMMC practice requirements

Our Reputation

As one of the first accredited C3PAOs, Kratos has over 25 years of extensive compliance and certification experience with government and commercial standards requirements including:

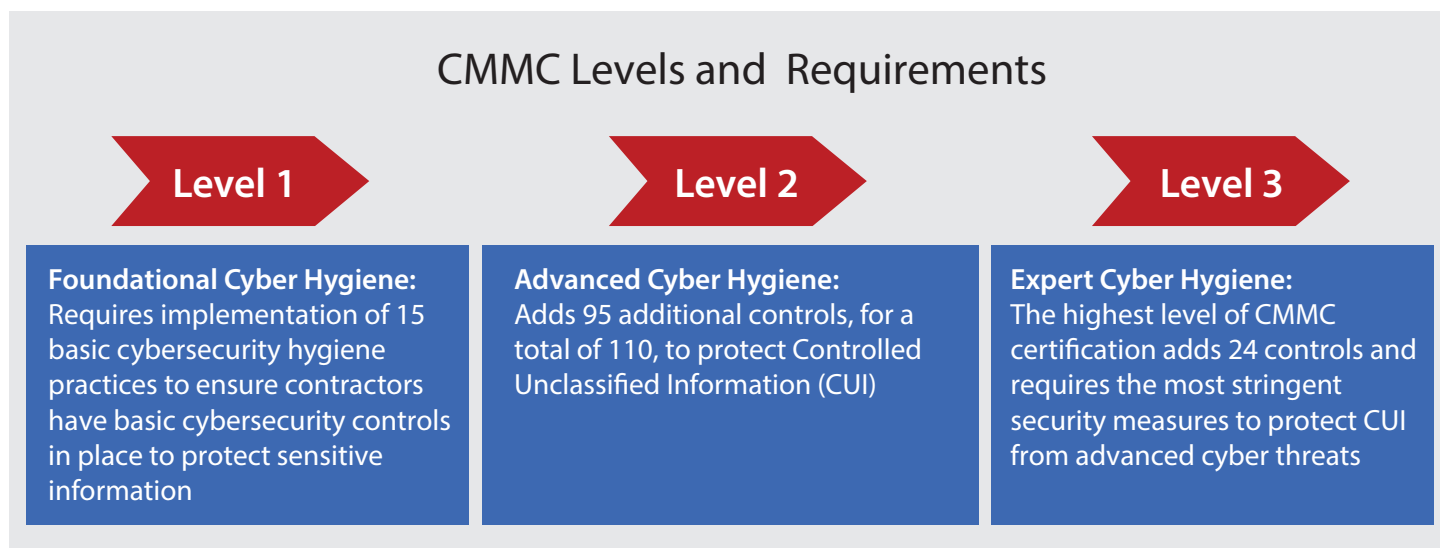
- Federal Risk and Authorization Management Program (FedRAMP)
- DoD Security Requirements Guide (SRG)
- ISO 27001
- HITRUST
- NIST Special Publication Series 800 & 1800
- StateRAMP

Strategic Industrial Base Security

As a leading authority on NIST-based standards, Kratos can evaluate compliance ahead of a formal assessment, provide specified consulting to address compliance gaps (technical and procedural), and develop needed documentation.

Three Levels of Cybersecurity Maturity

CMMC consists of 3 maturity level certification levels. Level 1 certification are self-assessments. Most Level 2 assessments require an assessment by a C3PAO. Finally, Level 3 assessments, which require Level 2 certification as a pre-requisite and are a delta assessment against only the Level 3 practices, are performed by the DoD, only.



Kratos is an accredited C3PAO and registered RPO. We are providing advisory support to many customers, have assessments of early adopters, and are continuing to schedule assessments of additional early adopters.