DFARS-CMMC Services

(405) 334-7305
Email | Web | Social

Why is CMMC important to my organization?

CMMC is vital to the success of your company as a member of the DIB for two reasons:

1) eligibility for government contracts
2) competitive advantage

Without CMMC, your organization will soon be ineligible to win any contract containing CUI.

At DCG, we work to streamline the CMMC preparation and certification processes, reducing your cybersecurity risk and helping to ensure your ability to win future DoD contracts.

Why do I need someone to help my company pursue CMMC?

Thoroughly and accurately assessing one's own cyber environment through the lens of hundreds of CMMC controls can be next to impossible. This is especially difficult for small and medium-sized businesses, because they often do not have dedicated cybersecurity staff-members. Employing an expert third-party contractor:

- **increases your likelihood of passing** a formal assessment the first time
- **reduces the risk of misinformation** or confused advice
- **streamlines the development of documentation**
- **provides a suite of experts** whose sole focus is your organization's compliance
- can be a **flexible, by-the-hour** engagement

Why DCG?

With more than 80 years of experience in the military and civilian cyber worlds combined, **Defense Cybersecurity Group is a trusted voice in the CMMC space**. Our trained staff partner with clients regardless of where they stand in their compliance journeys, bringing **technical expertise, real-world experience, and responsive leadership** to the CMMC certification process. Our team includes:

- **FBI InfraGard's Deputy National Sector DIB Chief**
- **Certified Cyber Professional Course Instructors**
- **Certified Cyber Professionals** (CCPs)
- **CMMC Provisional Assessors** (PAs)
- **CMMC Provisional Instructors** (PIs)
- **CCP Candidates**
- **Veterans with cyber warfare experience**

CEO Vince Scott

DEFENSE CYBERSECURITY GROUP

(405) 334-7305
Email | Web | Social

CMMC Road Map

PHASE 1: DISCOVERY MEETING

Regardless of your compliance status, every engagement will begin with a Discovery Meeting.

The goals of **Phase 1** include:

- to **better understand your organization's cyber environment**
- to **explore what Level of certification will be required** of your organization
- to **discuss which strategies would best fit** your organization's cyber and compliance needs

PHASE 2: JOURNEY DETERMINATION

The Journey Determination phase, which will be tailored to the needs of individual clients.

Phase 2 will consist of the:

- **creation of a high-level road-map** to prepare your organization for its CMMC journey
- **discussion of projected costs and timeframes**
- **reparation and education of key employees** in reference to FCI, CUI, and the requirements associated with the organization's required Level of CMMC compliance

PHASE 3: GAP ASSESSMENT

Gap Assessments review your cyber maturity in terms of DFARS/CMMC requirements.

Phase 3 will result in:

- **documented Basic-Self Assessment** and the production of **a SPRS Score**
- **definitive understanding of your cyber maturity** in terms of CMMC requirements
- **recommendations on how to proceed**, including how to best increase your SPRS score

PHASE 4: PROJECT MANAGEMENT

This phase will respond to the Gap Assessment conducted in Phase 3, the Basic-Self Assessment (BSA) conducted in Phase 5, and/or the Mock Assessment conducted in Phase 6.

Phase 4 will consist of the:

- development of **documentation**
- **technical and non-technical modifications** to your system architecture
- **selection of Service Providers**, such as SIEM/SOC Reps, or CSPs
- **return to Phase 3/5 as needed**

PHASE 5: BASIC SELF-ASSESSMENT

This phase is an iterative process. A BSA with a score of 110 is required before attempting a formal CMMC assessment.

Phase 5 will result in:

- **updated BSA score**
- **high-level understanding** of the current areas that require Plans of Action and Milestones (PoAMs) to meet requirements
- **understanding of your overall readiness** for CMMC assessment
- **return to Phase 3/4 as needed**

DEFENSE CYBERSECURITY GROUP

CMMC Road Map

(405) 334-7305
Email | Web | Social

PHASE 6: MOCK ASSESSMENT

This phase simulates a Level 2 assessment as though it were completed by a C3PAO and their team.

Phase 6 will consist of:

- DCG staff unfamiliar with the client's environment, or an external partner, will **conduct the mock assessment**
- **training of your employees** on what to expect from an assessment
- **DCG's expert coaching** throughout the assessment

PHASE 7: CERTIFICATION

At present, Cybersecurity Maturity Model Certification (CMMC) has not been fully implemented, and formal certifications cannot yet be conducted; they are anticipated to become required by October 1, 2025.

Regardless of what Phase 7 might look like for you, DCG's experts can still advocate for you, your architecture, and your team throughout the certification process.

If CMMC hasn't been finalized, why should I begin the certification process now?

The roots of Cybersecurity Maturity Model Certification (CMMC) reach back to the early 2000s. These requirements have been in the development and implementation phase for more than a decade. **The controls detailed in DFARS 7012 and NIST Special Publication 800-171 were required on a self-reporting basis in January of 2018. CMMC is the formal, third party assessment of these same requirements, and will be fully in effect in 2025.** We want the DIB to be prepared.

DFARS TIMELINE

2011

DFARS Case 2011-D039 introduces requirements for safeguarding unclassified information specifically as it related to fundamental research.

2013

DFARS 252.204-7000 Rule goes into effect providing guidance relating to the release of fundamental research.

2016

DFARS 7012+ goes into effect

2018

The implementation period for DFARS 7012 ends. The DoD position is that by entering a contract, a company is self attesting to satisfying DFARS 7012, and by extension the 110 controls of NIST 800-171.

2020

DFARS 7019 goes into effect as an interim rule requiring SPRS entries on DFARS 7012.

2020

DFARS 7020 goes into effect as an interim rule, a companion to 7019 that describes how to do the Basic-Self Assessment.

DFARS-CMMC Info

What is CMMC?

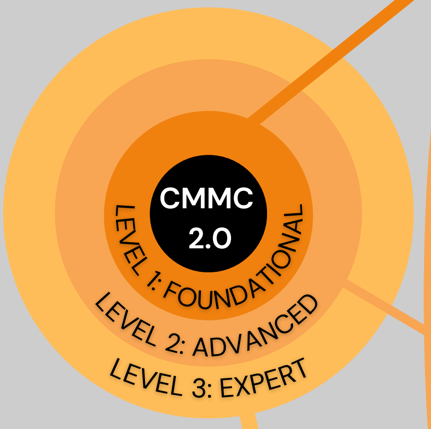
Cybersecurity Maturity Model Certification (CMMC) is a framework for cyber defense founded on the **DFARS 252.204-7012** and **NIST SP 800-171** documents. These mandates require all Department of Defense (DoD) contractors who handle **Federal Contract Information (FCI)** or **Controlled Unclassified Information (CUI)** to conform to the security controls introduced in NIST SP 800-171. In other words, the CMMC framework is a formal review which ensures NIST SP 800-171 controls are in place.

Federal Contract Information: FCI is information provided by or generated for the Government under contract not intended for public release

Controlled Unclassified Information: CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies excluding information that is classified under Executive Order 13526, and Classified National Security Information

Why has the DoD introduced CMMC?

The purpose of CMMC is to prevent the theft of intellectual property from the Defense Industrial Base (DIB), which has cost the U.S. economy billions in recent years. Many of the cyber requirements introduced in 2018 have been ignored by the DIB. CMMC is the DoD's way of ensuring controls which **prevent costly theft and malicious cyber attack** by foreign actors are systematically applied to their supply chain.



Level 1 includes **17 practices**, and applies to companies handling **FCI.**

Level 2 includes **110 practices**, and focuses on the protection of **CUI.** Currently, this requires an annual self-attested score to be submitted to the **Supplier Performance Risk System (SPRS)**. In the future, Level 2 will require a **Certified Third Party Assessment Organization's (C3PAO)** independent verification.

Level 3 has not been finalized, but will include Level 2 controls and controls from NIST SP 800-172. **Organizations Seeking Certification (OSCs)** will be assessed by government auditors triennially.

Click here *to see a short video about.* ***DFARS 7012, NIST 800-171****, and the* ***Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)*** *audit process.*