CMMC Readiness Services

For companies contracted with the Department of Defense (DoD), compliance with multiple Federal cybersecurity regulations can be a challenge.

The Cybersecurity Maturity Model Certification (CMMC) program is positioned to be the DoD's new seal of cyber-health for defense contractors bidding on federal contracts. As a streamlined standard, it is built upon adherence to Defense Federal Regulation Supplement (DFARS) clauses 252.204-7012, -7019, and -7020. By complying with the NIST SP 800-171 cybersecurity framework, defense contractors may satisfy existing DFARS requirements and forthcoming CMMC objectives and Contractual requirements – most notably safeguarding Federal Contract Information (FCI) and protecting Controlled Unclassified Information (CUI).

CMMC Overview

CMMC is a unified cybersecurity standard developed by the DoD to secure intellectual property and protected information (e.g., CUI) within the Defense Industrial Base (DIB). CMMC assesses three (3) levels of cybersecurity maturity within defense contractor organizations:

- Level 1: Foundational hygiene – 17 practices (FAR 52.204), protects FCI in non-critical programs
- Level 2: Advanced – 110 practices (NIST SP 800-171), protects CUI by acquisition prioritization
- Level 3: Expert – 110+ practices (NIST SP 800-172), protects CUI in critical national security programs

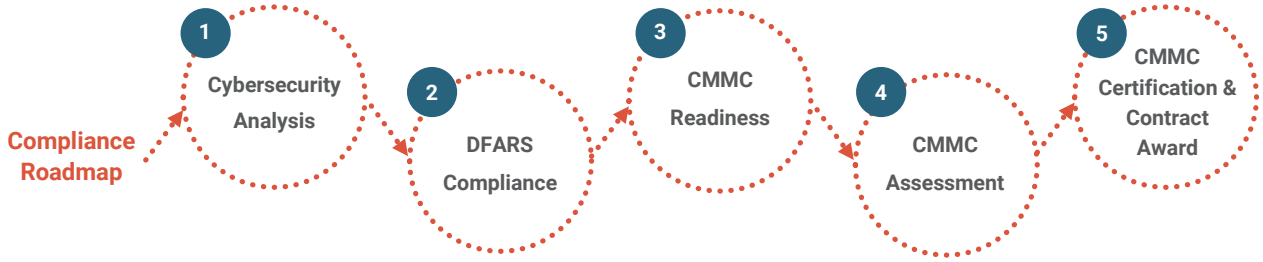
Beginning as early as the end of fiscal year 2022, all DoD contracts will include CMMC requirements based on defense program and acquisition prioritization, as well as defense contractor's ability to protect FCI and CUI. Thus, defense contractors must be certified at the specified CMMC Level (1, 2, or 3) provided by an acquisition at the time of contract award.

G2 Ops CMMC Readiness Services

As a CMMC Registered Provider Organization (RPO), G2 Ops is authorized by the CMMC Accreditation Body to provide tailored CMMC readiness and security compliance solutions. We guide Defense contractors through the process of maturing their cybersecurity capabilities and infrastructure to meet the DoD's cybersecurity compliance requirements as follows:

1. Perform a comprehensive cybersecurity analysis to measure organizational security hygiene and cybersecurity resiliency.
2. Navigate the NIST SP 800-171 and document organizational compliance with DFARS cybersecurity requirements.
3. Remediate identified gaps in security documentation and technology infrastructure while providing mitigation strategies to enhance the overall security program.
4. Deliver assessment preparation, scoping and evidence collection, and stakeholder training leading to formal CMMC assessment.

G2 Ops employs a consultative approach with focus on customized solutions for your company. We lead you to better understand the path to compliance while preparing your organization for CMMC.



G2OPS®

Smarter Intelligence.®

Arlington | Virginia Beach | San Diego | g2-ops.com | info@g2-ops.com | 1.757.965.8330