RADICL™
NEXT-GEN CYBERSECURITY-AS-A-SERVICE

CMMC Primer for DIB CEOs & Operations Leaders

WHAT IS CMMC?

Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's program requiring DIB contractors to prove they can protect sensitive information. It requires any defense company with a DoD contract to verify they're protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) in order to guard against potential cyber attacks.

WHY CMMC MATTERS NOW: 48 CFR

AFTER 11/10/26, LEVEL 2 C3PAO ASSESSMENTS BECOME REQUIRED

The Defense Department has formally integrated CMMC into federal contracting via a final rule in Title 48 CFR / DFARS, which became effective on November 10, 2025. This rule embeds CMMC requirements directly into solicitations and contracts, primarily through DFARS 252.204-7021, making cybersecurity a mandatory condition for contract awards.

CMMC IS GOVERNED BY TWO INTERLOCKING RULE SETS:

32 CFR Part 170
Which defines levels, assessment types, waivers, and program structure.

48 CFR / DFARS
Which makes those requirements contractually enforceable.

The DoD's phased rollout began on November 10, 2025, and will continue through 2028. Early stages include Level 1 and Level 2 self-assessments, while later stages introduce mandatory Level 2 assessments by a Certified Third Party Assessment Organization (C3PAO) and, ultimately, Level 3 certifications.

If a contract includes the CMMC clause and you lack the required status, you cannot be awarded the contract, regardless of pricing or past performance. This makes CMMC critically important for any contractor doing business with the DoD.

UNDERSTANDING FCI, CUI, AND CMMC LEVELS

FEDERAL CONTRACT INFORMATION (FCI)

FCI refers to nonpublic information provided by or generated for public information provided by or generated for the Government under a contract. It requires implementation of the 15 basic safeguarding controls outlined in FAR 52.204-21 and aligns directly with CMMC Level 1, which is satisfied through annual self-assessment and affirmation.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI is information requiring safeguarding under law, regulation, or governmentwide policy. It must be protected per the 110 controls outlined in NIST SP 800-171 R2, which forms the basis for CMMC Level 2. Depending on specific contract sensitivity, Level 2 may require a self-assessment or an assessment by a C3PAO.

HOW CMMC LEVELS MAP TO DATA HANDLING

LEVEL 1 (Foundational)	This protects FCI and no Plan of Action and Milestones (POA&M) are allowed. Level 1 requires annual self-assessment and executive affirmation.
LEVEL 2 (Advanced)	This protects CUI and requires full NIST SP 800-171 R2 implementation. POA&M are allowed only for certain items that carry a lower point value and have a mandatory 180-day closeout window.
LEVEL 3 (Expert)	This level is reserved for critical national security work and includes the same 110 controls from NIST SP 800-171 R2 as well as an additional 24 controls selected from NIST SP 800-172. Assessment is led by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

STEPS TOWARD CMMC READINESS

Drawing from DoD guidance and RADICL's expert insights, readiness should be treated as a continuous security program, not a one-time compliance project. CMMC compliance isn't just a checkbox to be addressed and moved past, but rather a new floor of acceptable cybersecurity practices for the future.

1. 

Define Scope

Within your organization, identify where FCI and CUI reside, which systems handle them, and which external service providers (MSPs, cloud platforms, SaaS tools) are in play. If needed, create a CUI enclave to reduce the assessment surface area.

2. 

Baseline Against NIST SP 800171 R2

Conduct a rigorous gap assessment using NIST SP 800171 R2, establish your Supplier Performance Risk System (SPRS) score, and develop both your System Security Plan (SSP) and POA&M. These documents determine your audit readiness and are mandatory for all contractors handling CUI.

3. 

Remediate Gaps (and Prioritize High-Risk Controls)

Leverage insights from your gap assessment to prioritize which controls need to be implemented, documented, and operationalized.

4. 

Build an Audit-Ready Evidence Package

Ensure policies, technical configurations, and implementation artifacts align to all 110 NIST SP 800-171 R2 practices. Evidence must reflect the environment exactly as it operates; mismatches are a common cause of audit failure.

5. 

Engage a C3PAO

Level 2 requires an assessment by a C3PAO, and your score will be automatically updated in SPRS. Levels 2 and 3 require three-year certifications plus annual affirmations. Level 1 requires that you register, self-assess, and enter your own score into SPRS, and requires an annual refresh.

6. 

Sustain Compliance Through Continuous Monitoring

Keep your security practices at the highest level with ongoing threat detection/response, vulnerability scanning, and change management. RADICL's industry-leading system blends managed detection with compliance workflows, meaning that your day-to-day security operations naturally produce audit evidence.

C3PAO CONSIDERATIONS

Verification

Only C3PAOs authorized by Cyber AB can perform Level 2 certifications. To pick an eligible assessor, you should confirm their marketplace listing, CAGE code, assessor credentials, and ISO17020 accreditation trajectory.

Impartiality

A C3PAO cannot consult for an organization it assesses, so you should always separate any Registered Provider Organization (RPO) advisory work from assessment work.

Assessment Logistics

Clarify scope, evidence format, onsite vs. remote testing, POA&M closeout expectations, and timelines for SPRS/eMASS submission. Naturally, demand is expected to spike as key RFP cycles approach, so it pays to be timely.

CONSEQUENCES OF NOT BEING CMMC CERTIFIED

CONTRACT INELIGIBILITY

Since November 10, 2025, contractors lacking required CMMC status are ineligible for any new contract where the clause applies. Phase 2 of CMMC rollout begins on November 10, 2026, at which point C3PAO Level 2 assessments will become a standard requirement.

AWARD TERMINATION & PROTEST RISK

If an apparent awardee lacks the required status or has not submitted the required affirmations into SPRS, competitors may file pre-or post-award protests, potentially disqualifying the awardee.

FALSE CLAIMS ACT LIABILITY

Organizations making inaccurate cybersecurity representations (such as inflated SPRS scores or unimplemented controls) risk damages, penalties, and public enforcement actions under the DoJ's Civil CyberFraud Initiative. Recent cases show multimillion-dollar settlements tied to cybersecurity misrepresentation, stressing the importance of not skirting around CMMC certification.

OPPORTUNITIES FOR CERTIFIED CONTRACTORS

PROTECTED REVENUE AND CONTRACT ELIGIBILITY

The most important consideration for DIB contractors is that CMMC certification ensures continued eligibility for DoD work and prevents supply chain exclusion.

COMPETITIVE ADVANTAGE

Primes increasingly filter potential subcontractors by their CMMC status, and certified firms gain preferential positioning and early-mover advantage as DoD enforcement expands. CMMC certification signals both trustworthiness and maturity in your operational security.

Ready to get started? Learn how RADICL can become your security operations and compliance partner, ensuring your CMMC readiness while directly addressing the hardest-to-meet requirements such as log management, vulnerability management, threat monitoring, and incident response.

CAICO
CMMC CERTIFIED ASSESSOR
CCA

RADICL™

Let's talk about how we can secure your organization.
RADICL.com/lets-talk-now