DORSEY
DORSEY+WHITNEY LLP

CMMC Phase 1 Begins November 10, Raising Complex Compliance and Enforcement Risks for Federal Defense Contractors

by Chris DeLong, Seth Goertz, and Alex Hontos

The Cybersecurity Maturity Model Certification program for federal defense contracts and solicitations is moving out November 10, 2025. This is just the start. CMMC implementation will happen in four phases over the next three years, reaching full implementation November 10, 2028. CMMC's compliance model will entail three tiers, each ramping up cybersecurity requirements and the number and character of representations and affirmations to the government. For prime contractors and subcontractors, CMMC raises new compliance and enforcement risks for organizations in the Defense Industrial Base. Read further for some topline information about CMMC and what it means for your organization.

Beginning November 10, the new DFARS CMMC solicitation provision, DFARS 252.204-7025, will be included in solicitations for applicable defense contracts. For now, contracts for commercially available off-the-shelf goods will remain excluded from the CMMC program. With the beginning of Phase 1, new solicitations and contracts will begin to require annual self-assessments and affirmations of compliance with 15 security requirements from Federal Acquisition Regulation (FAR) clause 52.204-21. Contractors and subcontractors will need to start reporting their self-assessments, assessments, and affirmations in the Supplier Performance Risk System (SPRS).

Parallel with the roll out of CMMC, the Department of Justice's Civil Cyber Fraud Initiative has announced new settlements and enforcement actions at an increasing pace in the last year, including where contractors affirmed compliance with CMMC requirements, which to date have been optional requirements for contracting officers to include in solicitations and contracts. Now, the broad sweep of federal defense contracts will have CMMC requirements and prime contractors and subcontractors in the Defense Industrial Base will face new compliance and enforcement risks.

What Is CMMC?

CMMC institutes a suite of cybersecurity practices and requirements to safeguard

Related People

- Chris DeLong
- Seth Goertz
- Alex Hontos

Related Capabilities

- Cybersecurity
- Government Enforcement & Corporate Investigations

sensitive government information, specifically Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), for contractors and subcontractors performing on defense contracts. The CMMC Model is tiered, with three levels of certification, each incorporating requirements from existing standards in FAR 52.204-21 and NIST SP 800-171 Revision 2. Level 1 is the baseline for cybersecurity hygiene, largely for organizations handling FCI, and requires annual self-assessment and affirmation of compliance with 15 security requirements from FAR clause 52.204-21. Level 2 ramps up requirements for organizations dealing with CUI, requiring either self-assessment or an assessment by a Certified Third-Party Assessor Organization (C3PAO) and affirmation of compliance with 110 security requirements in NIST SP 800-171 Revision 2. Level 3, the highest level, requires Level 2 C3PAO certification, an assessment by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), and annual affirmation of compliance with 24 identified requirements from NIST SP 800-171. Over the next three years, the CMMC Model will be implemented stepwise.

What Changes November 10 and Going Forward?

Starting November 10, Phase 1 introduces the Level 1 mandatory CMMC self-assessments for new solicitations and contracts. Contractors will not be able to win new business—or extend some existing contracts—without affirming Level 1 compliance. These must be affirmed and submitted in SPRS to remain eligible for covered contracts.

Phase 2 is slated for November 10, 2026, and will roll out the CMMC Level 2 requirements for applicable solicitations and contracts, including self-assessment and C3PAO certifications. Phase 3 is set for November 10, 2027, and CMMC Level 3 certification will be required for applicable solicitations and contracts. Phase 4, scheduled for November 10, 2028, will mark full implementation. All solicitations and contracts will include CMMC Level requirements and compliance will be a condition for contract award.

For CMMC Levels 2 and 3, contractors and subcontractors whose self-assessments or certification assessments identify lapses or requirements not met, Plans of Action and Milestones (POA&Ms) may be available. POA&Ms will afford contractors and subcontractors a conditional CMMC status while they address not-met requirements, with a 180-day closure deadline for deficiencies. Any POA&M not closed in time could result in expiration of the contractor's conditional status.

New Compliance and Enforcement Risks

DOJ's Civil Cyber Fraud Initiative, launched in 2021, has been ramping up. Using the False Claims Act as its hammer, the Initiative was created to ensure that government contractors and grant recipients follow required cybersecurity protocols. While still in its early days, DOJ has already signaled a willingness to enforce this new Initiative. Earlier this year, the Initiative announced settlements from a major defense contractor and a small business related to allegations that each had falsely certified compliance with CMMC requirements, which at the time were optional for contracting officers to include in solicitations and contracts. With the full roll out of CMMC, nearly all solicitations and

contracts will entail a minimum of a self-assessment and annual affirmation of compliance. These are new and complex compliance and enforcement risk vectors that organizations should assess carefully and plan for compliance.

Organizations that have not been thinking deeply about CMMC have to get oriented on the double. Winning future business, and even continuing to perform current work, may require significant effort evaluating your organization's current cybersecurity programs, practices, and plans and aligning them with CMMC's tiered requirements and planned roll out. Dorsey's cybersecurity and government contracts attorneys have the knowledge and experience to assist your organization.