PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

The Cybersecurity Maturity Model Certification Rule Has Been Published

By Thomas DeMayo, Partner and Nick DeLena, Partner

After half a decade in the making, the Cybersecurity Maturity Model Certification (CMMC) final rule has been published by the Department of Defense (DoD). The intent of the rule is to provide a verification mechanism for defense contractors' existing contractual cybersecurity obligations. The DoD seeks to ensure defense contractors have implemented required cybersecurity protections over Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) originating in Federal Acquisition Regulation (FAR) 52.204-21 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.

Background and Purpose

CMMC was first announced by officials at the DoD's Office of the Under Secretary of Defense's Acquisition and Sustainment group in 2019. As expressed in the 32 Code of Federal Regulations (CFR) § 170 rule, the DoD expects this final rule to protect DoD and the industry from the loss of FCI and CUI, including intellectual property.

In 2010, the value of U.S. intellectual property was estimated to be $5 trillion, with $300 billion stolen over networks annually, representing the greatest transfer of wealth in history. The rule states, "By incorporating heightened cybersecurity into acquisition programs, the CMMC Program provides the Department with assurance that contractors and subcontractors are meeting DoD's cybersecurity requirements and provides a key mechanism to adapt to an evolving threat landscape."

"This is critically important to the Department because defense contractors are the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing Defense Industrial Base (DIB) cybersecurity to meet these evolving threats and safeguarding the information that supports and enables our warfighters is a top priority for the Department. The CMMC Program is a key component of the Department's DIB cybersecurity effort."

What Companies Does CMMC Apply to?

The CMMC requirements will apply to any company holding cybersecurity obligations under FAR 52.204-21 and DFARS 252.204-7012. In our experience, not only does this include well-known major defense contractors, but companies in diverse industries including architecture, engineering, manufacturing, research and development, higher education and technology, among others. It does not matter whether these contractual obligations are in only one contract representing a small percentage of a company's revenue. As long as FCI or CUI are present in performance of the contract, CMMC requirements are likely to be present.

The CMMC framework consists of three levels:

Level	Applies To	Percentage of Defense Industrial Base It Applies To	Requirements
CMMC Level 1	Defense contractors in receipt of Federal Contract Information (FCI)	100%	Implement the 15 basic safeguards in FAR 52.204-21. Perform an annual self-assessment. An Affirming Official must attest to compliance annually.
CMMC Level 2	Defense contractors in receipt of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)	36%	Implement the 110 requirements and 320 underlying assessment objectives in National Institute of Standards and Technology (NIST) Special Publication 800-171r2. Most contractors subject to CMMC Level 2 requirements will need to hire a CMMC Third-Party Assessment Organization (C3PAO) to certify them to Level 2. Certifications are valid for three years. A small percentage, approximately 1.8 percent of the sector, will only be required to self-assess against Level 2. All contractors subject to CMMC Level 2 must have an Affirming Official attest to compliance annually.
CMMC Level 3	Defense contractors in receipt of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) *and* whose work or whose CUI is particularly sensitive to the Department of Defense	0.84%	Implement the 110 requirements and 320 underlying assessment objectives in NIST Special Publication 800-171r2. Obtain a CMMC Level 2 certification from a C3PAO. Certifications are valid for 3 years. Implement 24 additional requirements from NIST SP 800-172. Request a certification from the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) once the additional requirements are implemented.

When Does CMMC Go into Effect?

32 CFR § 170: introduces the compliance requirements from a cybersecurity and process perspective; published on October 15, 2024 and will go into effect 60 days later on December 16, 2024.

48 CFR § 252.204-7021: establishes the contractual clause and authority with which government contracting officers can place this rule into prime contracts; was published in a proposed state on August 15, 2024; the public comment period ended October 15, 2024 and the government is now in a period of rulemaking expected to conclude in mid-2025. Once 48 CFR § 252.204-7021 is published in final form, the CMMC program will go into effect.

CMMC Effective in Four Phases

Phase 1 – Begins on the effective date of the 48 CFR part 204 CMMC acquisition rule. DoD will include CMMC self-assessment requirements for all solicitations and as a condition of award.

Phase 2 – Begins one calendar year following the start of Phase 1. In addition to Phase 1 requirements, DoD intends to include requirements of CMMC certification for "applicable DoD solicitation and contracts."

Phase 3 – Begins one calendar year following the start date of Phase 2. In addition to previous requirements, DoD intends to include the requirement for CMMC certification for all DoD solicitations and contracts and as a condition to exercise an option period. This phase also includes CMMC Level 3 requirements for applicable contractors.

Phase 4 – Begins one year following the start of Phase 3.

Full implementation – DoD will include CMMC program requirements in all solicitations and contracts including option periods.

Changes Introduced in This Rule

The DoD has further clarified some aspects introduced in the proposed rule last year. That rule established definitions and requirements for Cloud Service Providers (CSPs) and External Service Providers (ESPs). Managed Service Providers (MSPs) who provide outsourced IT services are considered ESPs and under this rule are no longer required to obtain CMMC certifications in advance of their clients' efforts, so long as they do not store, process or transmit CUI on their clients' behalf. MSPs may choose to voluntarily obtain CMMC certification. ESPs that store, process or transmit their customers' Security Protection Data (SPD) will have their services in scope and be assessed as Security Protection Assets. If an MSP does not store, process or transmit CUI or SPD on behalf of their customers, they no longer meet the definition of an ESP.

Cloud Service Providers who handle only SPD are no longer required to obtain FedRAMP moderate authorization or equivalent. It is the Organization Seeking Assessment's responsibility to obtain a shared responsibility matrix from the CSP. The CSP's offerings should be assessed against relevant CMMC requirements. Cloud Service Providers that handle CUI on behalf of their customers must still obtain FedRAMP moderate authorization or equivalent from a FedRAMP 3PAO (Third-Party Assessment Organization).

Many defense contractors have implemented an enclave architecture separate from their enterprise networks for the storage, processing and transmission of CUI. A significant subset of those with enclaves have done so using a virtual desktop infrastructure (VDI) approach, whereby users access the enclave using remote desktop software from their enterprise, out-of-enclave computers. Prior to this rule, there has been only anecdotal guidance on how to treat the out-of-enclave endpoints that connect to the enclave. In this rule, the DoD has adjudicated that "an endpoint hosting a VDI client configured to not allow any processing, storage or transmission of FCI beyond the keyboard/video/mouse sent to the VDI client is considered out-of-scope. There are no documentation requirements for out-of-scope assets."

Repercussions of Non-Compliance

Defense contractors who fail to file CMMC self-assessments or fail to obtain CMMC Level 2 or 3 certifications will be ineligible to take award of solicitations with these requirements. In addition, misrepresentations or overrepresentations of your state of compliance in self-assessments may result in prosecution under the False Claims Act. Failure to annually affirm compliance in the intervening years between CMMC certifications will result in CMMC certificate cancellation.

Contractors' Critical Next Steps

Defense contractors with existing contractual obligations in FAR 52.204-21 (equating to CMMC Level 1) and DFARS 252.204-7012 (equating to CMMC Level 2) should continue to implement the requirements specified in those clauses. CMMC self-assessment requirements are expected as soon as the 48 CFR § 252.204-7012 rule goes final next year. It is critically important that contractors understand the entirety of what is required under these standards by referencing the companion assessment guides for both CMMC Levels 1 and 2. The assessment guides contain all of the detailed requirements an assessor will be looking for in a CMMC Level 2 certification context and represent the criteria to self-assess when your CMMC obligation is merely a self-assessment.

PKF O'Connor Davies Services for the Defense Industrial Base

PKF O'Connor Davies is a CMMC Third-Party Assessment Organization and Registered Provider Organization for the CMMC program. We assist companies in assessing their implementations of the requirements in the framework and help in addressing gaps by developing System Security Plans, policies and procedures; assembling artifacts; and building certification-ready documentation sets. Our years of experience with these requirements allow us to address our clients' strategic questions on overall investment in compliance and what constitutes cost-effective compliance strategies.

Contact Us

We welcome the opportunity to answer any questions you may have related to this topic or any other matters relative to cybersecurity and privacy. Please contact your PKF O'Connor Davies client service team or either of the Cybersecurity and Privacy Advisory team members below:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE, CMMC-CCP
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191