SQUIRE PATTON BOGGS

Navigating DoD's CMMC Program Final Rule

US – October 2024

On October 15, 2024, the U.S. Department of Defense (DoD) released its final rule to establish the Cybersecurity Maturity Model Certification (CMMC) Program (Final CMMC Program Rule).

The CMMC Program allows the DoD to verify that defense prime contractors and subcontractors (defense contractors) have implemented security safeguards for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) and are maintaining required safeguards during the contract period of performance. The CMMC requirements apply to defense contractors that process, store or transmit FCI or CUI in the performance of a DoD contract or subcontract.

In a parallel effort, the DoD also has proposed an acquisition rule – 48 C.F.R. Part 204 CMMC Acquisition Rule or (DFARS rule) – that will amend the Defense Federal Acquisition Regulation Supplement (DFARS) and contractually implement the CMMC Program (32 C.F.R. part 170) through DoD solicitations and contracts. In September we described the proposed DFARS rule, for which the comment period closed on October 15, 2024. The DoD estimates it will publish the final DFARS rule by mid-2025. The effective date of the final DFARS rule (which is 60 days after it is published in the Federal Register) is a key date, since that effective date will initiate the CMMC Program's phased rollout discussed below.

Background

The DoD designed the CMMC Program to protect FCI and CUI that it shares with defense contractors during contract performance. In 48 C.F.R. 52.204-21(a), FCI means "information, not intended for public release, that is provided by or generated for the Government under a contract ... but [does] not includ[e] information provided by the Government to the public (such as on public websites) or simple transactional information." In 32 C.F.R. 2002.4(h), CUI includes unclassified information that nevertheless requires safeguarding or dissemination controls based on a law, regulation or government-wide policy. CUI has different control levels (CUI Basic and CUI Specified) based on whether a federal agency has exercised a granted authority to require safeguarding or dissemination of the information.

The Final CMMC Program Rule does not change the definitions of FCI or CUI. It establishes a process by which the DoD can assess whether contractors and subcontractors that process, store or transmit FCI or CUI have achieved and maintain the appropriate CMMC level for the FCI or CUI that they handle.

Program Requirements

The Final CMMC Program Rule mandates compliance with one of three specified cybersecurity maturity levels based on the type and sensitivity of information handled by a defense contractor. The CMMC Program aligns Levels 1, 2 and 3 with the cybersecurity requirements described in 48 C.F.R. 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems) and National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171 Rev 2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) and 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171).

Program managers and requiring activities are responsible for selecting the CMMC status that will apply to a procurement and for setting the corresponding CMMC level based on a nonexhaustive list of factors, including (1) criticality of the associated mission capability; (2) the type of acquisition program or technology; (3) the threat of loss of the FCI or CUI in relation to the effort; and (4) impacts from exploitation of information security deficiencies.

The requirements for each CMMC Level are described below:

- **Level 1** – The defense contractor must implement the 15 security requirements set forth in 48 C.F.R. 52.204–21(b)(1)(i) through (xv), such as limiting system access to authorized users, controlling information processed on publicly accessible information systems, and updating cyber security protections as they become available.
  - The defense contractor must annually self-assess[1] its internal security controls to determine whether the controls are correctly implemented, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or the organization.
  - The contractor must meet all 15 Level 1 requirements without exception to achieve a CMMC status of Final Level 1. (As discussed below, Level 2 and Level 3 allow for a 180-day conditional certification).
  - The results of the annual Level 1 self-assessment are entered into the Supplier Performance Risk System (SPRS).
  - A 49-page CMMC Level 1 self-assessment guide is available.

1 Per the published DoD Chief Information Officer CMMC Level 1 self-assessment guide, a contractor can choose to perform the annual self-assessment internally or engage a third party to assist. Use of a third party to assist is still considered a self-assessment and does not result in a certification.

- **Level 2** – The defense contractor must comply with the 110 security requirements set forth in NIST SP 800-171 R2.
  - During implementation of CMMC Program Phase 1, a defense contractor must conduct a self-assessment to qualify to process, store and transmit CUI in the course of fulfilling a DoD contract.
  - Beginning in Phase 2 of the CMMC Program, a defense contractor must hire a CMMC Third-Party Assessment Organization (C3PAO) to conduct an assessment of its compliance with Level 2's 110 security requirements.
  - The defense contractor can shop for a C3PAO to engage on the CMMC Accreditation Body (AB) Marketplace (now doing business as The Cyber AB).
  - Certifications must be completed every three years and entered into eMASS (a government system accessible only to authorized users).
  - A defense contractor's Affirmation Official must complete an annual CMMC Program affirmation electronically in SPRS. (See Annual Affirmation section below).
  - A 246-page CMMC Level 2 assessment guide is available.
- **Level 3** – The defense contractor must achieve a CMMC status of Final Level 2 (C3PAO) before seeking CMMC status of Final Level 3 (DIBCAC).
  - To achieve a Level 3 certification, the defense contractor must first meet all requirements for Level 2 certification and an additional 24 requirements derived from NIST SP 800-172. The additional 24 requirements apply to CUI that is associated with a critical program or high-value asset.
  - The Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DCMA DIBCAC) must assess the contractor's implementation of the NIST SP 800-172 requirements.
  - A defense contractor's Affirmation Official must complete an annual CMMC Program affirmation electronically in SPRS. (See Annual Affirmation section below).
  - An 84-page CMMC Level 3 assessment guide is available.

CMMC Scoring Methodology

Unlike the CMMC Program Level 1 requirements discussed above, for CMMC Program Level 2 and Level 3, a defense contractor need not implement all requirements by its first assessment to be eligible for contract award. Specifically, for Level 2, if a defense contractor achieves a minimum required score on the assessment (i.e., 80% of the maximum score available), the contractor will achieve a CMMC status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO) as applicable. Each of the 110 security requirements will result in one of the possible findings – "MET," "NOT MET," or "N/A." Each requirement is weighted with a point value of 1, 3 or 5. For example, a requirement that, if not implemented, could lead to significant exploitation of a network is given a score of 5 points if MET and subtracted 5 points from the total if NOT MET. (N/A is given the same point value as if a requirement is MET.). A requirement that, if not implemented, has a limited or indirect effect on the security of the network and its data and receives a point value of 1.

To achieve a status of Conditional Level 2, a defense contractor must note all NOT MET requirements in a Plan of Action and Milestones (POA&M). A POA&M allows the contractor to obtain conditional certification for 180 days while working to implement the NOT MET requirements. A defense contractor cannot use a POA&M for a NOT MET requirement with a point value of 5. The contractor must implement the requirements in the POA&M within 180 days of receiving its Conditional CMMC Status to be verified with a second closeout assessment.

For Level 3, if the DCMA DIBCAC identifies that all 24 requirements from NIST SP 800-172 are satisfied, the contractor will have achieved a CMMC status of Final Level 3. A defense contractor achieves a CMMC status of Conditional Level 3 if the minimum score is achieved on the assessment (i.e., 80% of 24, or 19.2) and certain critical requirements are met. The contractor must note all remaining requirements in a POA&M. Unlike Level 2, the point values for Level 3 requirements are not weighted. With Conditional Level 3 status, the contractor satisfies the CMMC Program requirements for a contract award. Then, the contractor must meet the NOT MET Level 3 requirements within 180 days of receiving the Conditional CMMC Status as verified with a closeout assessment by DCMA DIBCAC. A POA&M closeout assessment will only assess NOT MET requirements carried over from the prior assessment. If the UNMET requirements are not MET within 180 days of the Conditional CMMC Status, then the conditional status will expire.

Risks for Failure To Comply With CMMC Requirements

Under the Final CMMC Program Rule, if a defense contractor operating under a status of Conditional Level 2 or Level 3 does not implement the NOT MET requirements to pass a closeout assessment within 180 days, then "standard contractual remedies will apply." These remedies are not defined in the Final CMMC Program Rule but may include contract termination, the government foregoing remaining contract options, and the government withholding progress payments.

Additionally, a defense contractor that fails to maintain the requirements of the applicable CMMC Program Level may face civil penalties under the False Claims Act (FCA). The Department of Justice (DOJ) launched its Civil Cyber-Fraud Initiative in 2021 to pursue government contractors that knowingly misrepresent their cybersecurity practices or protocols and that knowingly violate obligations to monitor and report cybersecurity incidents and breaches. The DOJ has used its authority under the FCA to bring suit against government contractors, including defense contractors, for failing to meet cybersecurity requirements. Accordingly, defense contractors should be aware of not only the contractual remedies but also the risk of civil penalties for not fulfilling CMMC requirements, since adherence to the CMMC Program will be included in the DFARS rule.

Annual Affirmation

In addition to the CMMC Program's assessment and certification requirements, a defense contractor must annually affirm continuing compliance with the CMMC Program's self-assessment or certification assessment (as applicable). Under § 170.4 of the Final CMMC Program Rule, the affirmation responsibility falls on the contractor's "Affirming Official," which means the "senior level representative ... who is responsible for ensuring [the defense contractor's] compliance with the CMMC Program requirements and has the authority to affirm ... [the] continuing compliance with the specified security requirements [Level 1, 2 or 3] for their respective organizations."

A defense contractor's Affirming Official responsible for compliance with the CMMC Program requirements must enter an annual CMMC Program affirmation electronically in SPRS and attest that the contractor has implemented and will maintain implementation of all applicable CMMC security requirements necessary to maintain either a Level 1, 2, or 3 certification.

Phased Rollout To Implement CMMC

DoD is rolling out the CMMC program in phases. The four phases of the implementation plan add CMMC Program requirements incrementally, starting in Phase 1 with self-assessments, and ending in Phase 4, which represents full implementation of the CMMC Program requirements. Beginning in Phase 4, eligibility for solicitations and resulting defense contracts involving the processing, storing or transmitting of FCI or CUI on a non-Federal system will require that the contractor have the required CMMC Program Level and assessment type.

Phase 1 – Begins on effective date of the DFARS rule, expected early-to-mid-2025. Phase 1 will last 12 months and would therefore end in early-to-mid-2026.

- **New solicitations and contracts** – Requirement for CMMC statuses of Level 1 (Self) or Level 2 (Self)2 for all applicable DoD solicitations and contracts as a condition of contract award.
- **Contracts in place prior to effective date** – DoD discretion whether to require CMMC status of Level 1 (Self) or Level 2 (Self) to exercise an option for solicitations and contracts awarded prior to effective date.

Phase 2 – Begins early-to-mid-2026 (one year after effective date of DFARS/start of Phase 1).

- **New solicitations and contracts** – CMMC Program status of Level 2 (C3PAO) for applicable DoD solicitations and awarded contracts, but DoD has discretion to delay the requirement to an option period instead of as a condition of contract award.
- DoD has discretion about whether to include the requirement for CMMC status of Level 3 (DIBCAC) for applicable DoD solicitations and contracts.

Phase 3 – Begins early-to-mid-2027 (one year after start of Phase 2).

- CMMC status of Level 2 (C3PAO) for applicable DoD solicitations and contracts as a condition of contract award and to exercise an option period on a contract awarded after the effective date.
- CMMC Status of Level 3 (DIBCAC) for all applicable DoD solicitations and contracts as a condition of contract award

Phase 4 – Begins early-to-mid-2028 (one year after start of Phase 3).

- Full implementation of the CMMC Program.
- No additional incremental requirements, DoD will include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

2 Under the Final CMMC Program Rule, the DoD has given itself discretion whether to require Level 2 (C3PAO) in place of the Level 2 (Self) CMMC Status during Phase 1.

Final CMMC Program Rule – Quick Look Table

CMMC Assessment Level	Covered Information	Level of Protection	Implementation Phase (estimated)*	Certification Authority	Certification Frequency	POA&Ms Permitted?	Cybersecurity Requirements
Level 1	FCI	Basic	Phase 1 (2025)	Self-assess in SPRS	Annual	No	NIST SP 800–171A Jun2018 (mapped from all 15 requirements of 48 CFR 52.204–21)
Level 2	CUI	General	Phase 1 (2025)	Self-assess in SPRS	Every three years	Yes	NIST SP 800-171 R2 (all 110 requirements as applicable)
Level 2	CUI	General	Phase 2 (2026)**	C3PAO certifies in eMASS	Every three years	Yes	NIST SP 800-171 R2 (all 110 requirements, as applicable)
Level 3	CUI	Enhanced	Phase 3 (2027)***	DIBCAC certifies in eMASS	Every three years	Yes	NIST SP 800-172 (24 additional requirements)

* Phase 4 (2028) represents "full implementation" of the CMMC Program but contains no additional incremental requirements.
** DoD intends to roll out C3PAO requirement for Level 2 certification as a condition of contract award in Phase 2 but, at its discretion, may delay inclusion of the requirement to an option period instead of as a condition of contract award.
*** DoD discretion whether to include DIBCAC requirement as early as Phase 2.

The Final CMMC Program Rule is effective December 16, 2024. Contractors that have not already been preparing to comply with CMMC are behind and need to play catch-up. Contractors need to immediately position themselves for continued success in working with the DoD through CMMC compliance. Check with this article's authors if you have any questions about CMMC compliance.

Contacts

Karen R. Harbaugh
Partner, Washington DC
T +1 202 457 6485
E karen.harbaugh@squirepb.com

Julia B. Jacobson
Partner, New York
T +1 212 872 9832
E julia.jacobson@squirepb.com

Genevieve B. Hubbard
Associate, Washington DC
T +1 202 457 6521
E genevieve.hubbard@squirepb.com

Patrick Madrid
Associate, Washington DC
T +1 202 457 5260
E patrick.madrid@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

squirepattonboggs.com

© Squire Patton Boggs. All Rights Reserved 2024

66688/10/24