wiley

ALERT

DOD Crystalizes CMMC 2.0 Program Rule

October 22, 2024

This alert was originally published on October 14, 2024, and last updated on October 22, 2024.

WHAT: On October 15, 2024, the U.S. Department of Defense (DOD) published the final CMMC 2.0 Program rule. DOD's final rule outlines the mechanisms that DOD will use to prescribe cybersecurity standards for safeguarding federal contract information (FCI) and controlled unclassified information (CUI), and to confirm that covered defense contractors and subcontractors have implemented the security requirements before award of covered contracts and are maintaining those safeguards during contract performance. The final rule details the tiered model of cybersecurity requirements DOD will use based on the type of information stored on a contractor's information system and the requirements for certifications and assessments based on the contract's assigned CMMC level.

WHEN: The final rule will take effect on December 16, 2024; however, CMMC's phased implementation will begin only after the related DFARS Acquisition rule takes effect. Comments on the proposed Acquisition rule closed October 15; over one hundred comments were submitted (we covered the proposed Acquisition rule here).

WHAT DOES THIS MEAN FOR INDUSTRY: When the CMMC Program rule and the complementary DFARS Acquisition rule are both finalized and in effect, DOD will begin its phased implementation plan in which contracting officers will assign a CMMC level and assessment type requirement to solicitations and resulting DOD contracts involving the processing, storing, or transmitting of FCI or CUI on a non-federal system. A contractor must meet the CMMC level, as confirmed by the appropriate assessment type, to be eligible for a contract award, unless the agency issues a waiver.

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Practice Areas

Cybersecurity

Government Contracts

Privacy, Cyber & Data Governance

CMMC 2.0 PROGRAM OVERVIEW

The final rule affirms the substantive security requirements from the proposed rule: Level 1 (15 security requirements in FAR 52.204-21); Level 2 (110 security requirements in the National Institute of Standards & Technology [NIST] SP 800-171 Rev. 2); and Level 3 (Level 2 requirements and 24 additional security requirements from NIST SP 800-172). The CMMC 2.0 Program will require contractors to periodically assess and annually affirm compliance to maintain CMMC status. The assessment frequency required is every year for a CMMC Status of Final Level 1, and every three years for a CMMC Status of Final Level 2 (Self), Final Level 2 (C3PAO), or Final Level 3 (DIBCAC), or when changes within the CMMC Assessment Scope invalidate the assessment. We discuss further below the guidance DOD provides in the final rule on the types of "changes" within the CMMC Assessment Scope that will require a reassessment.

Implementation Timeline

- **Phase 1**: After the CMMC Acquisition rule takes effect, Phase 1 begins. In the final rule, DOD extended the Phase 1 period from six months to one year. In Phase 1, DOD intends to include a requirement for CMMC Status Level 1 (Self) or Level 2 (Self) in all applicable DOD solicitations and contracts as a condition of award. Contracting officers will also have discretion to include a requirement for those statuses as a condition of receiving an option and to require CMMC Status Level 2 (C3PAO) in place of Level 2 (Self) for a specific contract or solicitation.
- **Phase 2**: The second phase will also last for one year. During Phase 2, DOD intends to include a requirement for CMMC Status Level 1 (Self), Level 2 (Self), or Level 2 (C3PAO) in applicable solicitations and contracts as a condition of award. Contracting officers will have discretion to delay the inclusion of a requirement for CMMC Status Level 2 (C3PAO) to an option period instead of as an award condition. Contracting officers may also choose to include the requirement for CMMC Status Level 3 (DIBCAC) in applicable DOD solicitations and contracts.
- **Phase 3**: The third phase will also last for one year. DOD intends to include a requirement for CMMC Status Level 1, Level 2 (Self), and Level 2 (C3PAO) in all applicable DOD solicitations and contracts as a condition of contract award and to exercise an option period; it will also include the requirement for CMMC Status Level 3 (DIBCAC) in all applicable DOD solicitations and contracts as a condition of award. Contracting officers will have discretion to delay the inclusion of a requirement for CMMC Status of Level 3 (DIBCAC) to an option period instead of as an award condition.
- **Phase 4**: Beginning three years from the effective date of the CMMC Acquisition rule, CMMC 2.0 will be fully implemented.

The final rule also reminds contractors that DOD may exercise an existing right to conduct a DCMA DIBCAC Medium or High assessment of a contractor's compliance with NIST 800-171 – in addition to CMMC Level 2 (Self) or Level 2 (C3PAO) assessments – as provided for under the DFARS clause 252.204-7020. We previously covered announcements about these assessments here.

CLARIFICATIONS IN THE FINAL RULE

Section 170.4 of the final rule includes definitions for key terms used throughout the text of the rule, to include "new terms and associated definitions, and customize[d] definitions for existing terms, as applied to the CMMC Program." Any CMMC-specific term is clearly marked with a "(CMMC-custom term)" identifier; the other terms include a citation reference to the source. A few of these terms that are of crucial importance for compliance are identified below:

- **Accreditation**: the status assigned to a person or organization that has met all criteria for the specific role they perform.
- **Assessment**: the testing or evaluation of security controls to determine whether the controls have been implemented correctly and are operating as intended. The required activities for each assessment depend on whether the assessment is for a Level 1, 2, or 3 or Plan of Action and Milestones (POA&M) closeout assessment and whether it is a self-assessment or certification assessment.
- **CMMC Status**: defined as achieving either a "Final" or "Conditional" Level 1, 2, or 3 status based on the company's ability to meet or exceed the minimum required score for each assessment level.
- **CMMC Status Date**: the date the CMMC Status assessment results are submitted. A new CMMC Status Date will not be assigned if a company moves from a "Conditional" to a "Final" assessment level.

In response to comments from interested parties, DOD also clarified a number of key terms and definitions. For example, DOD responded to comments seeking clarification about when reassessments would be required for certain system changes. DOD confirmed in the final rule that it does not anticipate requiring many reassessments and that they will only be "necessary when cybersecurity risks, threats, or awareness have changed, or indicators of cybersecurity deficiencies and/or non-compliance are present." Offering some relief to contractors, DOD stated that "adding or subtracting resources within the existing assessment boundary that follow the existing SSP [system security plan] do not require a new assessment."

Assessment Reciprocity

The final rule provides that a contractor that has achieved a perfect score on its Joint Surveillance Voluntary Assessment prior to December 16, 2024, the Program rule's effective date, will receive a Level 2 (C3PAO) status. The certification will remain active for three years from the date of the assessment so long as all required controls continue to be implemented.

Subcontractor Flowdowns

A CMMC level must be flowed down to subcontractors that will process, store, or transmit FCI or CUI. DOD provided a table summarizing the requirements for minimum subcontractor CMMC levels based on the CMMC level of the prime contract:

As expected, several commenters asked DOD to clarify how CMMC requirements should be flowed down to subcontractors. In the final rule, DOD clarified that when a subcontractor will process, store, or transmit CUI in performance of the subcontract and the prime contractor has, for the associated prime contract, a requirement of Level 2 (C3PAO), then CMMC Level 2 (C3PAO) is the minimum requirement for the subcontractor.

In response to comments, DOD also encouraged prime contractors to limit the flowdown of FCI and CUI to subcontractors when possible and noted that the procuring agency may specify additional guidance in solicitations. DOD reiterated that prime contractors are not required to assess subcontractor implementation of the requirements of NIST SP 800-171. However, they are required to flow down CMMC assessment requirements based on the type of information they expect subcontractors to receive, confirm that subcontractors have achieved the appropriate level, and refrain from disseminating FCI or CUI to subcontractors that do not meet the required CMMC level. DOD also stated that it expects contractors will share information about CMMC status with other defense industrial base members to facilitate effective teaming arrangements.

DOD declined to respond in this rulemaking to comments about the contractual language addressing subcontractor flowdowns, which was included in the Acquisition rulemaking (we covered the proposed rule here).

Joint Ventures

DOD declined to provide specific guidance for when contractors rely on systems controlled by other segments/businesses. In response to comments seeking clarification about how CMMC requirements apply to joint ventures, DOD reiterated that CMMC Program requirements will apply to information systems associated with contract efforts that process, store, or transmit FCI or CUI, that provide security protections for such systems, or information systems not logically or physically isolated from all such systems. DOD also stated that the "identity of an offeror or contractor as a joint venture does not in and of itself define the scope of the network to be assessed."

Cloud Service Providers (CSPs)

In the final rule, DOD also clarified some obligations for CSPs. For example, the final rule clarified that CSPs that process, store, or transmit CUI must comply with FedRAMP moderate or FedRAMP moderate equivalency in accordance with DOD Policy. CSPs that do not process, store, or transmit CUI do not need FedRAMP certification.

Incorporation by Reference

Contractors have previously asked DOD to clarify what security requirements the CMMC Program will utilize, particularly because NIST has published an update to Special Publication 800-171 and affirmed its intent to continue to update its publications about safeguarding CUI on federal and non-federal systems. In the final rule, DOD resolved some questions by identifying the specific guidance documents upon which CMMC security

requirements rely, including Revision 2 of SP 800-171. DOD left the door open to future updates to security requirements but foreshadowed that any updates would "u[se] the appropriate rulemaking process, to address evolving cybersecurity standards, requirements, threats, and other relevant changes."

NEW, HEIGHTENED FALSE CLAIMS ACT RISK

Recently, contractors have been facing increased scrutiny and risk of False Claims Act (FCA) liability arising from a knowing failure to comply with cybersecurity requirements or report cyber incidents. As we've written about in prior alerts, the Department of Justice has identified cybersecurity-related fraud as an area of enforcement focus with, among other things, the announcement of its Cyber-Fraud Initiative. Implementation of CMMC will only heighten those risks. For example, the annual affirmations of CMMC compliance required by covered contractors and subcontractors could be subject to the FCA. The individual making those affirmations must be senior and have responsibility for ensuring compliance with the CMMC requirements, which places a spotlight on those affirmations and their accuracy. Indeed, DOD highlighted these affirmations in its press release accompanying the CMMC final rule, and notably highlighted the rule's enforcement purpose: "CMMC provides the tools to hold accountable entities or individuals that put U.S. information or systems at risk by knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. The CMMC Program implements an annual affirmation requirement that is a key element for monitoring and enforcing accountability of a company's cybersecurity status."

In addition, contractors will be required to retain data from assessments for up to six years post-assessment. DOD affirmed that the organization seeking assessment will be responsible for determining "the best way to ensure artifact availability during the six-year retention period." DOD noted in the final rule that "the requirement for an artifact retention period of six years is a result of the Department of Justice's input to the proposed rule." Notably, the retention period mirrors the statute of limitations period under the FCA, which is six years from the date of a violation.

During the comment process, various parties raised concerns that the rule would increase FCA liability and requested different types of "safe harbors." In the final rule, DOD made no such accommodations, noting that DOD has no authority to change the FCA and that requests for a "safe harbor" were outside the scope of the rulemaking. Commenters also raised concerns about FCA liability arising from annual affirmations, which DOD also declined to address.

***

Wiley's cross-disciplinary Government Contracts, National Security, and Privacy, Cyber & Data Governance teams will continue to monitor these developments.