WINSTON & STRAWN LLP

BLOG

Be Prepared for CMMC Changes

OCTOBER 16, 2023

The Department of Defense (DOD) is expected to finalize a new rule by the end of 2023 that will significantly enhance the Cybersecurity Maturity Model Certification (CMMC) framework and related cybersecurity requirements for defense contractors. In November 2021, DOD released an advance notice of proposed rulemaking. This new rule, referred to as CMMC 2.0, is expected to be finalized by the end of 2023. CMMC is a unifying cybersecurity standard issued by the DOD that supports the common implementation of cybersecurity controls and safeguards across the entire DOD supply chain. CMMC is designed to enforce protection of sensitive unclassified information that is shared by DOD with its contractors, presently by classifying contractors into five progressive levels of cybersecurity maturity, from "basic" to "advanced." In order to qualify for contracts that include a requirement for CMMC compliance, contractors must meet the level of security required by that contract.

CHANGES IN CMMC 2.0

DOD issued the present cybersecurity framework (CMMC 1.0) in September 2020 as a response to the widespread failure of contractors to comply with self-assessments of their cybersecurity systems, and the DOD's inability to keep track of which contracts required contractors to maintain sensitive government information, as outlined in the DOD Inspector General's 2019 report. CMMC 1.0 classified contractors into one of five levels of security as determined by independent third-party assessments. While CMMC 1.0 has increased cyber security compliance by contractors, the requirement of third-party assessments has significantly increased costs, particularly for smaller contractors that handle non-sensitive information.

CMMC 2.0 will change the DOD's security requirements in the following three ways: (1) re-classify contractors into three levels of cybersecurity instead of five, (2) allow for contractors to conduct self-assessments to show compliance for select contracts with lower security requirements, and (3) allow for limited flexibility in compliance through plans of action and waivers.

Level 1, known as the "functional" level, will be for contractors that will be handling only Federal Contract Information (FCI), which is information that is not critical to national security. Contractors at this level will have to implement 15 basic information security safeguards that are outlined in FAR 52.204-21. To demonstrate compliance with these 15 safeguards, contractors need to complete an annual self-assessment of their cybersecurity systems combined with an attestation from a corporate executive affirming the results of the assessment. While self-assessments should

lower the cost of compliance, contractors should be aware that the reinstatement of self-assessments coincides with the Department of Justice's commitment to use the False Claims Act to pursue government contractors that misrepresent their compliance with cybersecurity standards.

Level 2, or "advanced," will be for contractors that transmit and store Controlled Unclassified Information (CUI).[1] To qualify for this level, contractors must comply with the 110 security requirements outlined in NIST SP 800-171, a guideline of cybersecurity practices set by the National Institute of Standards and Technology for contractors that require access to CUI. Importantly, NIST is expected to publish a new revision to SP 800-171 in early 2024 which will add new security requirements and thereby alter the ways in which contractors must comply. Assessments to demonstrate compliance with level 2 depend on the nature of the contract. For prioritized acquisitions, in which contractors send, share, receive, and store critical national security information, contractors must be assessed every three years by an independent CMMC Third-Party Assessor Organization (C3PAO). For non-prioritized acquisitions, contractors only need to complete an annual self-evaluation and attestation such as for contractors subject to the level 1 standard.

Level 3, or "expert," will be required for contractors with access to the highest-priority programs that use CUI. To qualify for this level, contractors must comply with 110+ security requirements contained in NIST SP 800-171, as well as its supplement NIST SP 800-172, which provides enhanced security requirements for the protection of highly sensitive data. To show compliance with level 3, contractors must pass a government-led assessment once every three years.

In limited circumstances, CMMC 2.0 will allow companies to receive contract awards prior to demonstrating complete compliance with a given level of cybersecurity, provided that the company has adequate plans of action and milestones (POAMs). DOD's intent is to specify a baseline number of requirements that contractors must achieve prior to the award of a contract, while allowing the remaining requirements to be addressed in a POAM with a clearly defined timeline.

CMMC 2.0 IMPLEMENTATION TIMELINE

DOD submitted the new version of CMMC to the Office of Information and Regulatory Affairs (OIRA) on July 24, 2023. OIRA review of the rule is limited to a maximum of 90 days. Once approved, the rule will be published in the Federal Register and will be subject to a 60-day public comment period. Absent OIRA finding a major flaw in the new rule, CMMC 2.0 is expected to be finalized before the end of 2023.

COMPLIANCE RECOMMENDATIONS

- Contractors should consider the following recommendations:
  - Understand the type of data the contractor processes for their existing contracts, or that will be required in new contracts.
  - Inventory and formalize the processes and controls that the contractor presently has in place to protect data.
  - Make a conservative estimate of the certification requirement that the contractor will be subject to and identify and correct gaps between the contractor's existing processes and controls and the estimated CMMC 2.0 requirements.

For further information or if you have questions, please contact the authors or your Winston & Strawn relationship attorney.

---

[1] NIST SP 800-171 Rev. 2, Appendix B at 72; *see also* NIST SP 800-171 Rev. 3 (Initial Public Draft), Appendix B at 72. CUI is defined as "[i]nformation that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended."

5 Min Read

Authors

Lawrence “Larry” Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Michael Hill

Related Locations

Washington, DC

Related Topics

Cyber Security

United States Department of Defense

Compliance

Government Contracts

Related Capabilities

Government Investigations, Enforcement & Compliance

Government Contracts

Related Professionals

Lawrence “Larry” Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Michael Hill

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.