Updates

The U.S. Department of Defense (DoD) has issued its long-awaited proposed rule implementing its Cybersecurity Maturity Model Certification (CMMC) program to protect sensitive, unclassified government information in the possession of defense contractors.

The rule sends a strong message to the Defense Industrial Base (DIB): If defense contractors want to do business with DoD, they will need to demonstrate their cybersecurity compliance, regardless of the size or type of company.

The 234-page proposed CMMC rule was published in the *Federal Register* on December 26, 2023, along with CMMC assessment guidance documents. The rule is not yet final and is open for public comment during a 60-day period that closes February 26, 2024. CMMC marks a significant milestone in DoD's efforts to strengthen

contractors' networks against cyber threats and protect against the loss of government information to adversaries. The rule lays the groundwork for a gradual rollout of CMMC requirements into new DoD contracts over several years. The rulemaking process is likely to generate significant input from industry and other stakeholders.

In this Update, we provide an overview of the proposed rule and its significance to contractors, as well as key issues to watch during the notice-and-comment rulemaking process.

CMMC: The Big Picture

Introduced in 2019 as an effort to move away from the "self-attestation" model of cybersecurity, CMMC is a three-tiered model intended to verify that contractors have implemented cybersecurity practices to manage Controlled Unclassified Information (CUI) and other data. CMMC's central requirement is that prime DoD contractors and subcontractors at all tiers must obtain CMMC certification at one of three levels as a condition for being eligible for a contract.

In September 2020, DoD published an interim rule implementing CMMC 1.0, which resulted in a CMMC contract clause set forth in the Defense Federal Acquisition Regulatory Supplement (DFARS) 252.204-7021. In November 2021, DoD announced CMMC 2.0, with proposed changes to streamline the model. CMMC 2.0 was then subject to an extensive internal review process within DoD with plans to subject the rule to a notice-and-comment rulemaking process.

According to DoD, it reviewed more than 750 public comments submitted regarding the interim rule as it prepared the proposed CMMC 2.0 rule. By issuing CMMC 2.0 as a proposed rule subject to public comment rather than an interim final rule that becomes immediately binding, DoD ensured that the rule would be subject to further public input before it is implemented.

Key Features of the Proposed Rule

CMMC 2.0 sets up a cybersecurity assessment regime using a three-level structure, each containing security requirements taken from existing cybersecurity regulations and guidelines applicable to government contracts under the FAR and DFARS.

- Level 1 will apply to defense contractors and subcontractors that process, store, or transmit Federal Contract Information (FCI), a broad category of nonpublic information that is provided by or generated for the government under a government contract. Companies subject to Level 1 will have to prepare a self-assessment verifying that they have implemented 15 basic security requirements that are required under FAR 52.204-21. A senior official from the company will be required to annually affirm continuing compliance and the results will be posted to DoD's Supplier Risk Performance System. Approximately 139,000 contractors will be subject to Level 1 during a seven-year phase-in period, according to the rule.
- Level 2 will apply to contractors that process Controlled Unclassified Information (CUI) on their information systems. CUI is unclassified information that requires safeguarding or dissemination controls pursuant to law, regulation, or governmentwide policy. As determined by DoD, contractors subject to Level 2 will need to either obtain a third-party assessment of their implementation of 110 controls in the National Institute of Standards and Technology's (NIST) Standard Publication (SP) 800-171 version 2 or instead be allowed to perform a self-assessment of their implementation of those controls. There is also a new affirmation requirement that requires a senior official of the contractor to affirm continuing compliance after every assessment and annually thereafter. Approximately 76,000 contractors will be subject to third-party assessments under Level 2 over seven years, according to the rule, while only 4,000 will be able to use self-assessments, according to DoD.

- Level 3 will apply to contractors with more sensitive, unclassified information that requires additional protections. In addition to satisfying the Level 2 requirements, they will need to implement 24 additional selected requirements from NIST SP 800-172. Level 3 assessments of contractors' implementation of those controls will be performed by DoD's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), which is part of the Defense Contract Management Agency (DCMA). As with Levels 1 and 2, a senior official of the contractor must affirm continuing compliance after every assessment and annually thereafter. Approximately 1,400 contractors will be subject to Level 3 certifications over a seven-year period, according to the rule.

According to the rule, DoD plans to introduce CMMC requirements in new solicitations over a three-year period. It estimates that it will take two years for companies with existing DoD contracts to become CMMC-certified. A CMMC certification for Level 1 will be valid for one year; certifications for Levels 2 and 3 will be valid for three years. However, contractors will be required to meet CMMC requirements during the performance of a contract period. They will also have to be prepared to make the newly required affirmations of compliance approved by a company "senior official" noted above, which raise new False Claims Act (FCA) risks for contractors and their executives. Attention to supporting documentation will be critical to mitigate risks.

The rule contains detailed cost estimates associated with obtaining CMMC assessments and submitting certifications. For example, it estimates that the cost of a Level 2 assessment under CMMC will be $117,768 over three years for nonsmall companies and $104,670 for small companies. But notably, the rule does not address the cost impacts to industry associated with staying compliant with existing cybersecurity requirements governing FCI and CUI set forth in FAR 52.204-21 and DFARS 252.204-7012. As the rule emphasizes, DoD presumes that contractors are already complying with requirements governing FCI and CUI and that "costs should already have been incurred and are not attributed to this rule." Contractors should bear in mind that any costs they incur related to assessments under CMMC will be in addition to the significant costs required to implement NIST SP 800-171, for example.

The proposed rule reaffirms DoD's reliance upon Certified Third-Party Assessment Organizations (C3PAOs) to perform third-party assessments of hundreds of thousands of companies under Level 2. The rule also reaffirms DoD's decision to delegate oversight of the training and accreditation of C3PAOs to the third-party, nongovernmental Accreditation Body (AB) because DoD determined that "there was insufficient capacity within the DoD to manage assessor training and assessments . . . ." As a result, the Cyber AB will play a significant role in matters such as C3PAO training and certification, assessment disputes, and avoiding conflicts of interest among C3PAOs. The Cyber AB also maintains a searchable marketplace that companies seeking CMMC will use to identify and select a C3PAO that they wish to use.

Key Issues To Watch

The proposed rule and accompanying guidance documents contain numerous details related to the scope of the rule and its application to hundreds of thousands of companies. Among the key aspects of the rule are the following:

- Plans of Action and Milestones (POA&Ms)—a document maintained by a contractor that describes how and when any unimplemented security requirements will be met—will be permissible for CMMC Level 2 only. But such unimplemented controls are time-limited; they must be closed out within 180 days of an initial assessment. POA&Ms also will not be allowed for CMMC Level 1.
- Prime contractors will be required to flow down the CMMC clause to subcontractors and ensure that it is further flowed down to lower-tiered subcontractors.
- Notably, the Level 2 requirements are tied to version 2 of the NIST SP 800-171 controls, notwithstanding the fact that NIST has recently issued version 3 of NIST SP 800-171. There also appears to be a risk of

inconsistent requirements between CMMC and the existing clause at DFARS 252.204-7012(b)(2)(i), which in its current state requires contractors that handle CUI to implement the version of NIST SP 800-171 "in effect at the time the solicitation is issued or as authorized by the Contracting Officer."

- Contractors will be able to achieve a CMMC Level for their entire enterprise network or specific enclaves, depending on where the information to be protected is located. The rule explains that companies must be capable of maintaining security requirements at the requisite CMMC Level "regardless of the business size" of the company. Also, there is no exception for foreign contractors or subcontractors of U.S. prime contractors.
- The rule addresses various details regarding the scope and application of CMMC assessments. For example, Internet of Things (IoT) devices, Operational Technology (OT) systems, and other such specialized assets will not need to be assessed against CMMC security requirements for Levels 1 or 2, but for Level 2, such assets are required to be documented in a company's System Security Plan (SSP). For Level 3, such assets will be assessed against CMMC Level 2 security requirements.
- The rule states that DoD may elect to waive application of CMMC third-party assessments in particular procurements. But the rule states that there is no process for companies to request a waiver of CMMC requirements.
- The rule establishes requirements for resolving disputes related to assessments. Each C3PAO will be required to have a time-bound, internal appeals process to address disputes related to a perceived error, malfeasance, or unethical conduct by the assessor. Disputes regarding assessments that cannot be resolved by a C3PAO will be escalated to the Accreditation Body, whose decision will be final. Questions about which CMMC Level applies to a contract will be directed to the Contracting Officer. Given that CMMC certification at the requisite level will be a requirement for any DoD contract, it is reasonable to expect that CMMC-related issues will arise in bid protest litigation.
- The rule contains important new details relevant to contractors that outsource IT and cybersecurity functions to an external service provider (ESP) or commercial cloud service provider. Significantly, according to the rule, if a contactor uses an ESP, the ESP must have a CMMC certification at the CMMC Level that is equal to or greater than the level sought by the contractor. This provision has significant ramifications for defense contractors and managed service providers that provide IT and other such support. The rule does not explain how CMMC certification of an ESP is supposed to be achieved. Under existing regulations, CMMC certification is only available to a defense contractor. If a contractor uses an external cloud service provider to process, store, or transmit CUI, it must ensure that the CSP's products or services are either authorized as FedRAMP Moderate or High or meet requirements equivalent to those baselines.

Final Thoughts and Recommendations

Although the rule is subject to change, the release of CMMC 2.0 is a major development. The rule is among several regulatory developments demonstrating that cybersecurity is increasingly becoming a competitiveness issue for contractors in the defense and civilian agency markets.

Notwithstanding the rollout of CMMC 2.0 over several years, contractors should not delay in examining the rule, evaluating its impact on their businesses, and making the necessary investments. Among other things, companies should consider taking the following actions:

- Conduct gap assessments of their networks against NIST SP 800-171 controls as applicable, seeking expert assistance as needed.
- Review and regularly update cybersecurity policies and procedures, including System Security Plans, in anticipation of CMMC and other pending regulatory developments.
- Consider implementing procedures to delegate responsibility to appropriate officials within the company as necessary to obtain and submit self-attestations of compliance to DoD.

- Continue to be mindful of the FCA risks associated with false or misleading attestations related to cybersecurity, as highlighted by recent cases and settlements under the U.S. Department of Justice's (DOJ) Civil Cyber-Fraud Initiative. FCA risks should also be considered when company officials prepare and sign off on the attestations of compliance required by CMMC. Indeed, FCA actions may be brought against individual company executives as well as companies for alleged false claims.
- Consider strategies to engage with suppliers and teaming partners with the recognition that CMMC will apply at all tiers of the defense supply chain.

Authors

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Explore more in

Government Contracts Privacy & Security

Related insights

Update

FDA Food Import and Export Updates for Industry

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights