GT GreenbergTraurig

Alert | Government Contracts

January 2024

DoD Issues Proposed CMMC Rule for Contractors

Go-To Guide:

- If the Department of Defense (DoD)'s Proposed Rule is finalized, solicitations for defense contracts would, in most cases, assign a Cybersecurity Maturity Model Certification (CMMC) level and require a cybersecurity assessment for contractors to be eligible for contract award.
- Organizations holding Federal Contract Information (FCI) would be required to self-assess annually against 15 cybersecurity controls in NIST SP 800-171 rev. 2 and mandated by FAR 52.204-21.
- Organizations holding Controlled Unclassified Information (CUI) would, at a minimum, be required to self-assess every three years against the 110 controls in NIST SP 800-171 rev. 2. Some organizations would be required to obtain a third-party assessment of compliance with the 110 controls in NIST SP 800-171 rev. 2. Others may be required to obtain Level 3 CMMC Certifications for information systems holding sensitive CUI. The Level 3 certification is completed by DoD and requires compliance with the 110 controls in NIST SP 800-171 rev. 2 and 17 controls from NIST SP 800-172.
- Comments on the proposed regulations are due Feb. 26, 2024. Contractors should not expect significant changes to the Proposed Rule or the ability to recover implementation costs.

On Dec. 26, 2023, DoD published a proposed rule implementing the CMMC Program (the Proposed Rule). The regulations come more than three years after the release of the initial CMMC regulations (November 2020) and two years after the Biden administration announced the revised "CMMC 2.0"

program (January 2021). The Proposed Rule largely reflects the CMMC 2.0 version of the program, although there are important details and clarifications added in the over-200-page rule.

Since 2015, the Federal Acquisition Regulation (FAR) has required contractors to comply with 15 basic safeguarding cybersecurity controls, and in 2017, a DoD clause required all defense contractor information systems which stored, processed, transmitted, or developed covered defense information or controlled technical information to comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. However, neither of these clauses provided a mechanism for DoD to verify contractor compliance with either of these standards. Based on findings in a 2019 DoD Inspector General (IG) Report, DoD learned that most DoD contractors were not consistently implementing these mandatory security requirements. The IG Report recommended that DoD implement mechanisms to verify contractor compliance, and DoD introduced the CMMC Program in 2020.

The Proposed Rule would implement changes to Title 32 of the Code of Federal Regulations and add a new Part 170 to authorize and describe the CMMC program. The Proposed Rule does not include revisions to the Defense Federal Acquisition Regulation Supplement (DFARS), which are required prior to the program's finalization and effective date.

CMMC Program Fundamentals

As indicated by DoD's CMMC 2.0 announcement, there are three CMMC levels. The tiered model requires that companies implement controls at progressively advanced levels, depending on the type and sensitivity of the information they possess. The core of the model is an assessment requirement, which allows DoD to verify the implementation of cybersecurity requirements. As a condition of contract award, the information systems containing the covered information will need to be certified at the CMMC level specified in the solicitation, and retain that certification, with no gaps, for the life of the contract. Prime contractors will also be required to ensure subcontractor compliance throughout the supply chain at the applicable CMMC level for each contract. Because the focus is on protecting government information, a single solicitation may require different CMMC certifications for different aspects of performance, or a single entity may hold multiple CMMC certifications depending on the number of information systems and the nature of the information contained within those systems.

- Level 1 Self-Assessment: Level 1 requires an annual self-assessment of all contractor information systems that contain FCI. The security requirements for Level 1 are those set forth in FAR 52.204-21(b)(i)-(xv). For assessment purposes, each requirement has been tied to a NIST SP 800-171 rev. 2 control, and the associated assessment methodology in NIST SP 800-171A can be used to determine whether the control is met. No plans of action and milestones (POA&Ms) are allowed, and each control must be "met" under the assessment methodology for the entity to have completed the certification requirements. After the completion of the self-assessment and annually thereafter, the entity must affirm its continued compliance with Level 1 security requirements.
- Level 2 Self- or Certification Assessment: For entities with information systems containing CUI, either a self-assessment or a third-party assessment against all 110 controls in NIST SP 800-171 rev. 2[1] is

[1] Note that all controls are based on NIST SP 800-171 rev. 2, or NIST SP 800-172. The rule states that DoD's "requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 Rev 2 and NIST SP 800-172 requirements. Additional rulemaking may be necessary in the future to conform CMMC requirements described in this rule to any changes in the underlying information protection requirements defined in the foundational NIST guidelines." 88 Fed. Reg. 89058, 89074 (Dec. 26, 2023). Thus, the rule contemplates that if the CMMC Program changes the standards to address (upcoming) revisions to NIST SP 800-171, it will be done through a formal rulemaking process. This approach raises questions about compliance with the CMMC standards and other cybersecurity regulations, such as DFARS 252.204-7012, that rely on the "current version" of the NIST standards. DoD has indicated it will update the -7012 clause this year, through which process it may harmonize the language of these requirements.

required. The self-assessment must be completed by the entity, and the certification must be obtained from an authorized CMMC assessment organization (C3PAO). POA&Ms are acceptable for some controls, but only if they are resolved within 180 days and if the assessment score divided by the total number of security requirements is greater than or equal to 0.8. The assessment must be conducted in accordance with the assessment methodology in NIST SP 800-171A, which requires that a control be fully implemented to be considered "met." At the completion of the self- or certification assessment and annually thereafter, the entity must submit an affirmation attesting to its continued compliance with Level 2 security requirements. Affirmations are also required following any POA&M closeout activities.

- Level 3 Certification Assessment: For entities with information systems containing certain types of CUI, DoD may require the organization to meet additional security controls. Prior to seeking a Level 3 Certification Assessment, an organization must already have obtained a Level 2 Certification Assessment. Any Level 2 POA&Ms must be closed prior to the initiation of the CMMC Level 3 Certification Assessment. The government will assess a contractor's compliance with the 110 controls in NIST SP 800-171, and 17 additional controls from NIST SP 800-172. At the completion of the government assessment and annually thereafter, the entity must submit an affirmation attesting to its continued compliance with Level 3 and Level 2 security requirements. Affirmations are also required following any POA&M closeout activities.

Level 2 Certification Assessments will be conducted by a C3PAO that has been accredited by the CMMC Accreditation Body (AB). Level 3 Certification Assessments will be conducted by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). If an entity disputes the findings of an assessment organization, each assessment organization must have an internal dispute process managed by individuals within the assessment organization not involved in the original assessment activities. If a dispute cannot be resolved using this internal process, it will be escalated to the AB, whose decision is final.

Implementation

The Proposed Rule contemplates a phased approach to CMMC implementation, with requirements initially being included in solicitations based on availability of C3PAOs. The Proposed Rule lays out a four-phased approach to implementation:

- Phase 1 would begin on the effective date of the CMMC revision to DFARS 252.204-7021 (not yet released). During this phase, DoD would include Level 1 or Level 2 self-assessment requirements in applicable solicitations and contracts as a condition of contract award. DoD may include Level 2 Certification Assessment requirements, i.e., assessments by C3PAOs rather than self-assessments, in some solicitations and contracts. DoD may also include such requirements prior to exercising an option on a contract awarded prior to the effective date.
- Phase 2 would begin six months following the start date of Phase 1. DoD would begin including Level 2 Certification Assessment requirements in all applicable solicitations and contracts. DoD may delay the inclusion of Level 2 Certification Assessment requirements to an option. DoD may also, at its discretion, begin including Level 3 Certification Assessment requirements in applicable solicitations and contracts.
- Phase 3 would begin one calendar year following the start date of Phase 2. During this phase, DoD intends to include Level 2 and Level 3 Certification Assessment requirements in all applicable solicitations and contracts as a condition of contract award. For Level 2, DoD would also include the Certification Assessment requirements as a condition to exercise an option period on a contract

awarded prior to the effective date. DoD may, in its discretion, delay the inclusion of Level 3 Certification Assessment requirements for exercising an option.

- Phase 4 would begin one calendar year following the start date of Phase 3. This phase would constitute full program implementation. DoD would include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

Consequences of Non-Compliance

Failure to comply with the CMMC requirements or maintain compliance with the applicable controls in the CMMC level can result in revocation of the CMMC level. The CMMC Program Management Office (PMO) would be responsible for investigating and acting upon indications that an active CMMC self-assessment or certification assessment has been called into question. An investigation may be triggered based on information from the CMMC Accreditation Body or an assessment organization. If the CMMC PMO determines that any requirements of the applicable level have not been achieved or maintained, a revocation of the contractor's CMMC status is possible. In such cases, standard contractual remedies would apply, and the entity would no longer be eligible for additional awards at the CMMC level that has been revoked. In addition, the assessments and affirmations require entities to make numerous representations about the status of their cybersecurity practices and procedures. Misrepresentations or false statements made during these activities could also give rise to False Claims Act liability, or investigations by the Department of Justice, which has an active Civil Cyber-Fraud Initiative.

Contractors that have not been diligently managing their cybersecurity compliance with FAR and DFARS requirements and working toward compliance with the NIST SP 800-171 controls may want additional time to achieve compliance or may desire to pass along the costs of becoming compliant to DoD. DoD has, however, been clear in the rulemaking process that the CMMC requirements reflect, and are aligned with, information security requirements that have been mandatory since at least December 2017. In DoD's view the underlying obligations have applied far longer than that. Therefore, contractors should not expect significant changes to the Proposed Rule or the ability to recover costs of becoming compliant with the existing FAR and DFAR cyber standards embodied in the Proposed Rule.

What Can Contractors Do Now?

Comments on the Proposed Rule are due Feb. 26, 2024. Interested contractors should plan to submit comments on areas of concern or places where further clarification is required. Given the impact of the new rule, it is likely that DoD will receive extensive comments from interested parties. Once the comments have been received and reviewed, the government must respond to each comment, explaining why it has or has not made a corresponding change in the Proposed Rule. This is likely to take some time. Additionally, the same process will need to occur for the yet-to-be-released changes to the DFARS.

In the meantime, for companies wishing to get ahead of CMMC implementation, the Joint Surveillance Voluntary Program (JSVA) may provide an opportunity to be assessed against the controls in NIST SP 800-171 prior to the implementation of the CMMC program. An authorized assessment organization works with DIBCAC to perform an assessment against the NIST SP 800-171 controls. An organization that has completed this assessment, with no open POA&Ms, is eligible to receive a CMMC Level 2 final certification, valid for a three-year period following the voluntary assessment.

Authors

This GT Alert was prepared by:

- Eleanor M. Ross | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- Cassidy Kim | +1 415.590.5133 | Cassidy.Kim@gtlaw.com
- Jeffery M. Chiow | +1 202.331.3149 | Jeff.Chiow@gtlaw.com