wiley

ALERT

UPDATE: DOD Proposed Rule Solidifies Plans for CMMC 2.0 Program: Security Requirements, Assessments, Affirmations, and Some Flow-Down Details

January 11, 2024

WHAT: The U.S. Department of Defense (DOD) has issued a proposed rule setting forth key requirements for its long-anticipated Cybersecurity Maturity Model Certification (CMMC) 2.0 program. The proposed rule primarily addresses security, assessment, and affirmation requirements for contractors that handle federal contract information (FCI) and controlled unclassified information (CUI). DOD also released drafts of eight CMMC program guidance documents that further describe assessment processes and provide key scoping guidance. We've previously covered anticipated changes from the CMMC 1.0 program here.

WHEN: DOD issued the proposed rule on December 26, 2023, with a 60-day comment period (through February 26, 2024).

WHAT DOES THIS MEAN FOR INDUSTRY: Although it may not change the substantive security controls that 99% of contractors must implement, the proposed rule will require significant additional compliance steps for virtually all companies that do business with the Department of Defense, whether as prime contractors or subcontractors. For most companies, these new steps include affirmations and third-party certifications to prove that the company complies with existing security measures (chiefly, FAR 52.204-21, which requires contractors that handle FCI to implement certain basic security controls, and DFARS 252.204-7012, which requires contractors that handle CUI to implement the additional security controls in NIST SP 800-171 Rev 2). For those few companies that work on certain

Authors

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance
Telecom, Media & Technology

programs that DOD designates as critical or that handle high-value assets, the proposed rule would require the company to also implement more significant security controls prescribed in NIST SP 800-172 and undergo a separate assessment by the government's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

We lay out the nuts and bolts of the program, including the security requirements, assessments, affirmations, scoping, timing, flow downs, and other key takeaways below. For a big picture look at what requirements might apply to each of your contracts, we've also developed a flowchart.

OVERVIEW

At long last, DOD has released its updated CMMC 2.0 rulemaking. DOD designed the CMMC Program to require contractors and subcontractors to demonstrate that any sensitive data that they handle – particularly FCI and CUI – is adequately safeguarded.

The CMMC Program is intended to: (1) align cybersecurity requirements to the sensitivity of unclassified information to be protected; (2) add a self-assessment element to affirm implementation of applicable cybersecurity requirements; (3) add a certification element to verify implementation of cybersecurity requirements; and (4) add an affirmation to attest to continued compliance with assessed requirements. As part of the program, DOD also intends to provide supporting resources and training to the Defense Industrial Base (DIB) to help support companies that are working to achieve the required CMMC Level. The CMMC Program provides for assessment at three levels, starting with basic safeguarding of FCI at CMMC Level 1, moving to the broad protection of CUI at CMMC Level 2, and culminating with higher-level protection of CUI against risk from Advanced Persistent Threats (APTs) at CMMC Level 3.

The CMMC Program will require DOD (specifically, program managers and requiring activities) to identify CMMC Level 1, 2, or 3 as a contract requirement for any effort that will cause a contractor or subcontractor to process, store, or transmit FCI or CUI on its unclassified information systems. A separate rulemaking, DFARS Case 2019-D041, will further define contracting processes for CMMC, including how DOD will select and identify the required CMMC Level in new solicitations and existing contracts.

Who must comply with CMMC? At least some component of the proposed rule would apply to all defense contractors and subcontractors that will process, store, or transmit FCI or CUI on their information systems. As part of its Regulatory Impact Analysis, DOD estimated that this would include about 220,000 companies, the vast majority of its supply chain.

In response to several questions it received in response to the previous CMMC 1.0 program, DOD clarified that this rule will not extend to "Internet Service Providers or telecommunications service providers (i.e., common carriers)" because DOD does not consider their networks to be part of the contractor's information system or their relationship to be that of a subcontractor. Instead, DOD explained that it expects contractors and subcontractors to encrypt any CUI before transporting it across a common carrier's network. Of course, a common carrier could separately qualify as a defense contractor or subcontractor by providing other services

directly to DOD or as a subcontractor to another prime contractor.

DOD also included an exception for contracts or orders that are exclusively for commercially available off-the-shelf (COTS) items or are valued at or below the micro-purchase threshold.

How will DOD communicate CMMC requirements? Once the proposed rule is finalized, DOD will communicate two items in any solicitations for contracts involving FCI or CUI on a non-Federal system, each of which is discussed more below: (1) a CMMC Level, which establishes the security controls that the contractor must implement; and (2) the type of assessment required to verify that the contractor has implemented the required security controls. The proposed rule states that, once applicable, offerors must satisfy both requirements to be eligible for a contract award, although a separate rulemaking, DFARS Case 2019-D041, will further define contracting processes for CMMC. The proposed rule states that DOD program managers or requiring activities will be responsible for selecting the CMMC Level that applies to a particular procurement based on the type of information (FCI or CUI) that will be processed, stored on, or transited through a contractor information system.

What are the requirements for each CMMC Level? And can contractors use POA&Ms to meet them? The proposed rule provides for three different sets of security controls, which correspond to the three levels: basic safeguarding of FCI at Level 1, broad protection of CUI at Level 2, and enhanced protection of CUI against risk from APTs at Level 3. As DOD previewed, the proposed rule also outlines parameters for time-bound plans of action and milestones (POA&Ms), which may be allowed for certain security controls under Levels 2 and 3. In its Regulatory Impact Analysis, DOD also revealed its expectations as to what share of the 220,000 companies affected by the eventual final rule will be subject to each level.

> **Level 1:** Requires compliance with 15 security requirements identified in FAR clause 52.204–21, with which many contractors are already familiar. DOD anticipates that Level 1 will apply to almost 140,000 entities (roughly 63%).
>
> **Level 2**: Requires compliance with DFARS 252.204-7012 security requirements, the 110 security requirements listed in NIST SP 800-171 Rev. 2.
>
> The proposed rule notes that a PO&AM may be allowed for certain security requirements if three conditions exist: (1) the assessment score divided by the total number of security requirements is no less than 0.8; (2) none of the security requirements in the PO&AM have a value of greater than 1 (as specified in the CMMC Scoring Methodology); and (3) the security requirements in the PO&AM do not include any of the five requirements that are prohibited to have a PO&AM (as identified in the rule). When allowed, POA&Ms must be closed — and verified by follow-up assessment — within 180 days of the initial assessment. This may present scheduling challenges because contractors will need to rely on their assessor to closeout the assessment during that period.
>
> Notably, unlike the current DFARS 252.204-7012 clause, the proposed rule specifically references ***Revision 2*** of NIST SP 800-171, which means that CMMC will not automatically incorporate NIST's planned Revision

3; DOD will retain control over when and how the changes in that Revision impact DOD contractors.

DOD anticipates that Level 2 will apply to over 80,000 entities (roughly 36%).

Level 3: Requires compliance with the Level 2 requirements and 24 select requirements from NIST SP 800-172. Like in Level 2, a PO&AM is only permitted if the assessment score divided by the total number of security requirements is no less than 0.8; and the PO&AM does not include one of the seven Level 3 requirements that are prohibited to have a PO&AM (identified in the rule). DOD anticipates that Level 3 will apply to roughly 1,500 entities (roughly 1%). The POA&M closeout timeline may be even more challenging for this level because the contractor will need to rely on DIBCAC to complete its follow-up assessment in the 180-day period.

What are the different assessment types? The proposed rule discusses three types of assessment: (1) Self-Assessment (used for Levels 1 and 2), (2) Certification Assessment by a Certified Third-Party Assessor Organization (C3PAO) (used for Level 2), and (3) Certification Assessment by DIBCAC (used for Level 3).

Self-Assessment (Levels 1 and 2): When a contract requires CMMC Level 1 or, in some limited situations, Level 2, contractors may assess their own compliance through a Self-Assessment process. For Level 1, contractors will be required to complete this Self-Assessment annually. When a Self-Assessment is sufficient for Level 2, contractors will be required to complete the assessment every three years. Of the 80,000 contractors that DOD anticipates will be subject to Level 2, DOD anticipates allowing a Self-Assessment for only 4,000 once DOD has fully implemented the program. During the first six-month implementation phase (discussed more below), however, DOD may allow many more contractors to conduct a Self-Assessment because DOD plans to rely primarily on Self-Assessments during Phase 1. But if C3PAO capacity allows for it, many contractors may be better off obtaining a Certification Assessment to avoid the risks that could occur if a C3PAO later disagrees with the contractor's Self-Assessment.

C3PAO Certification Assessment (Levels 2 and 3): For most contracts requiring CMMC Level 2 and all contracts requiring CMMC Level 3, contractors must obtain a Certification Assessment. A Certification Assessment must be conducted by a C3PAO, which the contractor is responsible for retaining. The C3PAO will verify that the contractor has implemented the 110 security requirements in NIST 800-171, Rev. 2. Contractors will be required to obtain this Certification Assessment every three years.

DIBCAC Certification Assessment (Level 3): When a contract requires CMMC Level 3, a contractor must also undergo a second assessment by DIBCAC. DIBCAC will verify that the contractor has implemented the 24 additional security controls from NIST SP 800-172. DIBCAC may also "perform checks" of CMMC Level 2 security requirements; note that all Level 2 PO&AMs must be closed prior to initiating a Level 3 Certification Assessment. Contractors will be required to undergo this assessment every three years as well.

What other representations or affirmations are required? In addition to completing the assessments discussed above, contractors will be required to affirm their compliance to DOD at specific intervals, including upon completing an assessment, closing out a PO&AM that may derive from an assessment, and on an

annual basis thereafter. Affirmations must be completed by a senior official from the contractor.

How broadly throughout my organization do these requirements apply? The proposed rule emphasizes the importance of scoping the information system(s) that will be subject to these requirements, and those scoping rules vary depending on the applicable CMMC Level. These scoping rules determine what information system assets contractors should include as they develop their System Security Plans (SSPs) and prepare for an assessment; they also clarify the degree to which certain assets are assessed. As DOD notes in the proposed rule, a contractor may scope its information system to include its entire enterprise environment, or it may include only an enclave or subset of information system assets. This all depends on how and where contractors handle (or plan to handle) FCI and CUI.

> **Level 1:** Contractors can limit the information system to only those assets that process, store, or transmit FCI.
>
> **Level 2**: Contractors must include — and assess against all security requirements — all assets that process, store, or transmit CUI and all assets that provide security functions to in-scope assets. At Level 2, contractors must also identify certain "contractor risk managed assets" that are not physically or logically separated from CUI assets and "specialized assets," such as Internet of Things devices and operational technology, but contractors need not assess these latter two categories against all the security controls required for Level 2. Contractors should document contractor risk managed assets and specialized assets in their asset inventory and SSP. An assessor may conduct a limited check of contractor risk managed assets if the contractor's risk-based security policies, procedures, and practices documentation raise questions.
>
> **Level 3:** Contractors must include all four categories referenced above for Level 2 and assess all security requirements against assets in all four categories. Because these rules for scoping differ, contractors that intend to eventually pursue CMMC Level 3 will need to apply the Level 3 Scoping Guidance when preparing for their Level 2 Assessments.

How will DOD phase its implementation? DOD anticipates that it ultimately will require a CMMC Level as a condition of awarding new contracts and as a condition of exercising an option period in existing contracts (which could constitute a change and require further negotiation). To accomplish that end, DOD anticipates a phased implementation over three years. The implementation period would consist of four phases:

> **Phase 1 (Months 0 – 6)**: Starting on the effective date of the revision to DFARS 252.204-7021, which has not yet occurred, DOD intends to include Level 1 or Level 2 Self-Assessments in all applicable DOD solicitations and contracts as a condition of award. DOD may, at its discretion, include a Level 2 Certification Assessment requirement instead of a Level 2 Self-Assessment requirement. DOD may also include Level 1 or Level 2 Self-Assessment requirements as a condition to exercise an option period on a contract awarded prior to the effective date of the DFARS -7021 revision.
>
> **Phase 2 (Months 7 – 12)**: Six months after Phase 1 begins, DOD intends to include a Level 2 Certification Assessment requirement in applicable solicitations and contracts as a condition of award. DOD may opt

to wait to include the Certification Assessment requirement in an option period instead of including it as a condition of contract award. DOD may also, at its discretion, include a Level 3 Certification Assessment requirement. As DOD expands the requirement for Certification Assessments in this phase, it may require a contractor that had just completed a Self-Assessment during Phase 1 to undergo a Certification Assessment in Phase 2 a few months later. Thus, contractors should not assume that any designations made in one phase are permanent, and contractors should be mindful that any Self-Assessment they conduct could be followed shortly by a C3PAO Certification Assessment.

Phase 3 (Months 13-24): One year after Phase 2 begins, DOD intends to include a Level 2 Certification Assessment requirement in all applicable solicitations and contracts as a condition of award and a condition to exercise an option period on a contract awarded prior to the effective date of the DFARS -7021 revision. DOD also would include a Level 3 Certification Assessment requirement in all applicable solicitations and contracts, but it may opt to wait to include the Level 3 Certification Assessment requirement in an option period instead of including it as a condition of contract award.

Phase 4 (Months 25+): One year after Phase 3 begins, DOD will include CMMC program requirements in all applicable solicitations and contracts, including option periods on contracts awarded before Phase 4 began.

Are prime contractors required to flow down these requirements? The proposed rule would require prime contractors to flow down CMMC Program requirements to subcontractors that also will process, store, or transmit FCI or CUI in performance of the subcontract. DOD states that CMMC Level requirements will apply to subcontractors "throughout the supply chain at all tiers" that will process, store, or transmit FCI or CUI on contractor information systems in performance of the contract or subcontract. The proposed rule establishes the minimum CMMC Level for a subcontractor based on the prime contractor's CMMC level and whether the subcontractor will process, store, or transmit only FCI (Level 1) or CUI (Level 2 Self-Assessment). If the prime has a Level 2 or Level 3 Certification Assessment requirement and the subcontractor will process, store, or transmit CUI, the subcontractor will be required to have at least a Level 2 Certification Assessment. Still, the proposed rule is not a model of clarity and does not state whether a prime will ever need to require a subcontractor to achieve a level above the minimum requirement.

What happens if a dispute arises between a contractor and its assessor? The rule references an appeal process for CMMC assessments. DOD explained that the process is derived from ISO/IEC 17020:2012 and ISO/IEC 17011:2017. For contractors that wish to appeal a C3PAO Certification Assessment, DOD requires each C3PAO to have a time-bound, internal appeals process to address disputes. Contractors would send requests for appeal to the C3PAO, which will have individuals who were not involved with the original assessment review the request. If unresolved at the C3PAO level, contractors would elevate the dispute to the Accreditation Body, whose decisions will be final. Contractors may also appeal DIBCAC Certification Assessments, which will be reviewed by DIBCAC.

* * * *

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