6 Steps To Ready Defense Contractors For Cybersecurity Rule

By **Sandeep Kathuria** (November 1, 2024)

Sandeep Kathuria

Effective Oct. 15, the U.S. Department of Defense made progress toward effectuating the Cybersecurity Maturity Model Certification by publishing a final rule establishing CMMC in federal regulations.[1]

CMMC would create a third-party certification regime to validate that defense contractors are meeting the 110 security requirements imposed via DOD regulations[2] for protection of controlled unclassified information[3] on the contractors' information systems.

In place of getting a third-party CMMC assessment, defense contractors that do not handle controlled unclassified information would be required instead to self-assess and attest that they have met the 17 basic safeguarding controls in the Federal Acquisition Regulation — a subset of the 110 requirements — to protect federal contract information.[4] While CMMC has been beset with delays in the more than five years since it was conceived by the DOD, the establishment of CMMC as a federal program means that it likely will be moving forward.

One regulatory step remains. To implement CMMC in government contracts, the DOD must complete rulemaking to add CMMC requirements in solicitation provisions and contract clauses in the Defense Federal Acquisition Regulation Supplement.

According to the DOD, the final rule establishing CMMC in defense contracts and subcontracts is expected in the first half of 2025.[5] CMMC should be fully implemented by 2028 based on the DOD's phased rollout plan.

This article provides a refresher about CMMC and identifies best practices for CMMC readiness, focusing on key issues affecting defense contractors.[6]

How did we get here?

As of Dec. 31, 2017, the DOD required defense contractors to implement the security requirements in National Institute of Standards and Technology, or NIST, Special Publication 800-171 via a contracts clause found at DFARS 252.204-7012 that is included in most defense contracts and other transaction agreements. With limited exceptions, this clause also must be flowed down to subcontractors throughout the defense supply chain.

However, to date, the DOD has considered contractors and subcontractors to comply provided that each entity developed a system security plan, maintained a plan of actions and milestones, or POA&M, for each requirement not met,[7] and completed a cybersecurity self-assessment in the supplier performance risk system for each information system used in contract performance.[8]

CMMC would change existing practice and eventually require defense contractors to implement all 110 NIST controls on all their information systems that process, store, or transmit controlled unclassified information for the DOD during contract performance. However, there will be flexibility built into the CMMC model to account for temporary deficiencies, enduring exceptions to compliance, and POA&Ms will still be permissible in the

near term.

Once CMMC is implemented, cybersecurity will become foundational to doing business with the DOD at any tier.

What is the CMMC model and levels?

CMMC has three levels. The DOD program managers or requiring activities shall determine which level applies for a procurement based on the information handled on the contractor information system.[9]

At Level 1, defense contractors need to meet the 17 basic safeguarding requirements identified in the Federal Acquisition Regulation, or FAR, to protect federal contract information.[10] However, POA&Ms are not permitted.

At Level 2, contractors ultimately must meet all 110 security controls in NIST SP 800-171 Revision 2 due to processing of controlled unclassified information in contract performance. For contractors that have not met all requirements, it still will be possible to obtain a conditional CMMC certificate to remain eligible for award, but such contractors (1) must meet an assessment score of 80% based on CMMC scoring methodology, i.e., 88 points, (2) may not have POA&Ms for certain controls, and (3) must close out deficiencies within 180 days as verified in a POA&M closeout assessment.[11]

If these conditions are met, the contractor can achieve conditional CMMC status despite not immediately implementing all requirements. If any POA&Ms are not closed in 180 days, however, the conditional status will expire, and the contractor temporarily will be ineligible for future contract awards under CMMC, and there may be contractual repercussions for previously awarded contracts.[12]

While some Level 2 procurements will allow for self-assessment, most contractors will need an independent assessment.

Level 3 has the same requirements as Level 2 but adds 24 technically complex and expensive security requirements from NIST SP 800-172, enhanced security requirements for protecting controlled unclassified information, a supplement to NIST Special Publication 800-171. The DOD will be responsible for assessing the implementation of these 24 requirements instead of a third-party assessor.

When achieved, CMMC status is effective for three years.

What are the exceptions and variations to CMMC?

For special circumstances or systems that do not allow for all DOD cybersecurity requirements to be met, such as regarding medical devices and test equipment, defense contractors may use an "enduring exception" to a security requirement.[13] While a plan of action is not required, the special circumstance must be documented in a system security plan along with mitigations, and it will be scored as though the contractor met the requirement.[14]

Likewise, the DOD has confirmed that contractors temporarily can be out of compliance with a security requirement without losing CMMC status. This may occur due to a "temporary deficiency," which is a condition where remediation of a discovered deficiency is feasible, and a known fix is available or is in process.[15] The deficiency must be documented in an

operational plan of action to include details on progress toward implementing corrections or reducing or eliminating vulnerabilities. However, contractors will remain eligible for contract awards despite the deficiency.[16]

In a key change, the DOD has will permit government program managers to seek advance approval to waive inclusion of CMMC in solicitations/contracts. This waiver may apply to a specific procurement or class of procurements.

However, the DOD has stated that such a waiver may occur in very limited circumstances and must be approved by a service acquisition executive or component acquisition executive in the DOD, and it remains to be seen whether this authority will be used.

How does CMMC apply to the supply chain and the use of cloud services?

Just as with the DFARS cybersecurity clause found at 252.204-7012, CMMC will have a flow-down requirement imposed on prime and higher tier contractors. While purchases of exclusively commercially-off-the-shelf items and purchases below the micro-purchase threshold will be exempt, all other subcontracts including those for commercial products or services will be subject to CMMC.[17]

The prime or higher tier contractor will be required to ensure the supplier has the CMMC certificate or self-assessment required before subcontract award.

The DOD may provide guidance pertaining to flow-down to subcontractors in the solicitation and at the specified level.[18] In the absence of such guidance, prime contractors may need to determine which level applies to the work being performed by subcontractors.[19] However, the appropriate level may not always be clear.

Defense contractors may use cloud service offerings to handle controlled unclassified information but must ensure that the cloud service provider meets the Federal Risk and Authorization Management Program moderate baseline or equivalent requirements.[20] Additionally, the contractor's on-premises infrastructure connecting to the cloud service provider's product or service offering must be assessed for CMMC purposes.[21] This must be documented in the contractor's system security plan.

What are contractors' ongoing compliance obligations?

Under the new CMMC program rule, an affirming official[22] from each defense prime and subcontractor must affirm its organization's continuing compliance after every successful CMMC assessment, "including PO&AM closeout, and annually thereafter," and enter this affirmation in supplier performance risk system.[23] This new requirement should prompt defense contractors to develop additional policies to ensure that such affirmations will be made accurately.

The DOD also may conduct a CMMC status investigation of a defense contractor that has achieved CMMC status and certification.[24] If the investigation finds that the contractor has not properly implemented or maintained security requirements, the DOD may use contractual remedies and the contractor will be ineligible for future contract awards until new CMMC status is achieved.

Any contractor misrepresentation of its compliance also could lead to liability for the contractor under the False Claims Act under the U.S. Department of Justice's civil cyber-fraud initiative.

What should my company be doing to get ready for CMMC?

Companies that work with the DOD, either directly or indirectly, should make sure they are on track for CMMC certification or a self-assessment as applicable.

If a CMMC requirement is included in a solicitation, task/delivery order, or as a condition to exercise an option period, then affected prime contractors will need to meet the CMMC level identified therein at contract award for Level 1 and no later than six months after award for Level 2.

Subcontractors will have corresponding obligations if they handle federal contract information or controlled unclassified information. Defense contractors and subcontractors risk loss of potentially all their business with or for the DOD if they wait too long to make the necessary investments for CMMC.

While a comprehensive CMMC readiness list is beyond the scope of this article, defense contractors and subcontractors should consider the following.

1. Assess the scope of CMMC and identify which company information systems will be covered.

Initially, contractors should understand what assets will be assessed. The DOD's updated scoping guidance should be reviewed.[25]

Contractors should identify all covered information systems. It may be necessary to catalog which systems have controlled unclassified information/federal contract information to understand how many systems will be affected by CMMC.

For larger organizations with significant involvement in defense contracting, the affected systems may go beyond the corporate enterprise network and include systems that are not managed or even known by the IT organization. It will be important to ensure CMMC readiness for all contractor information systems with controlled unclassified information/federal contract information.

2. Develop plans to address any gaps in implementation of NIST SP 800-171 or FAR 52.204-21 for covered systems, and shore up existing security documentation.

As part of CMMC planning, contractors should ensure that any POA&Ms are scheduled to be closed before a third-party assessment and be prepared to open new plans of action to address any deficiencies that are found while preparing for CMMC. Additional investments may need to be made in the contractor's 2025-2026 IT budgets.

Additionally, if gaps are found, contractors should investigate the facts and take appropriate remedial actions, particularly if there were potential misrepresentations of cybersecurity compliance to the government. Security documentation also may need to be updated.

3. Identify and vet third-party CMMC assessors and negotiate pricing and terms and conditions.

There is a significant shortage in capacity for CMMC assessments. Currently, there are only 58 approved third-party assessors for CMMC, and there are approximately 78,000

companies that will need at least one assessment over the next three to four years. Many companies will need numerous assessments. The supply cannot keep up with the demand.

It would be prudent for defense contractors to find a qualified CMMC assessor and to lock in pricing for assessment(s) in 2025 or beyond. Market forces will influence the cost of a CMMC assessment, and the price will go up, potentially substantially.

4. Seek verification or assurances from suppliers that they will be able to meet CMMC when it is a flow-down requirement.

Prime and higher tier contractors often need to be able to field a team for large procurements. If their suppliers will be processing controlled unclassified information or federal contract information, then these suppliers will need to have met their respective CMMC requirements. Prime contractors will need to plan to ensure that their key suppliers will have timely met CMMC.

This could be a competitive differentiator for large contractors and integrators. Contractors that manage cyber supply chain risk effectively will have an advantage in future procurements.

5. Engage with government customers and program managers about procurements that may include a CMMC requirement in the near future.

Business development and legal and contracts teams will need to understand CMMC and find out if/when it will be a requirement in the near term on upcoming contracts.

Such advance planning will be critical in the early days of CMMC. This planning will enable the contractor to determine which information systems will be covered and to be ready for CMMC in a particular solicitation and contract.

If a company cannot meet CMMC or lacks sufficient compliant suppliers, then it may instead need to shape upcoming solicitations to exclude CMMC and/or advocate for an agency waiver.

6. Prepare a plan for internal review and validation of CMMC affirmations and mechanisms for ongoing review and oversight of cybersecurity compliance.

The role of the affirming official will be key for organizations. It should be someone sufficiently knowledgeable about cybersecurity.

Companies should develop processes in advance for compliance reviews before any affirmation of compliance are submitted to the government or a prime contractor. Such a process also should include checks and balances.

Related to affirmations of compliance, it is important to ensure employees are heard if they disagree about whether a security requirement has been met. The right answer may not always be clear as cybersecurity involves judgment and there is often more than one way to meet a requirement.

Defense contractors should not ignore concerns, however, and review and adjudicate questions that come up. Particularly because of the DOJ's cyber-fraud initiative and its reliance on employee whistleblowers, it is important for defense contractors to have a clear record of cybersecurity compliance.

Sandeep Kathuria is senior counsel at Ice Miller LLP.

[1] https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program.

[2] See DFARS 252.204-7012(b)(2).

[3] The DoD uses the term "Covered Defense Information" in DFARS 252.204-7012, which is the term that the DoD initially established in 2016 to describe the information requiring protection. More recently, the DoD instead has been using the term that applies government-wide, which is "Controlled Unclassified Information." Although there is a distinction between these terms, this article will use "Controlled Unclassified Information" for the purpose of simplicity as defined in 32 CFR 2002.4(h).

[4] See 32 CFR 170.22(b)(1). Federal Contract Information is defined in FAR 52.204-21.

[5] https://www.defense.gov/News/Releases/Release/Article/3932947/cybersecurity-maturity-model-certification-program-final-rule-published/.

[6] This article does not address the role of private-sector businesses and other entities comprising the CMMC assessment and certification ecosystem.

[7] See Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61505, 61508 (Sept. 29, 2020). A Plan of Action and Milestones is a document that identifies tasks needing to be accomplished. See 32 CFR 170.4.

[8] See DFARS 252.204-7020.

[9] See 32 CFR 170.3(d).

[10] The safeguarding requirements are in FAR 52.204-21.

[11] 32 CFR 170.21(a) and (b).

[12] 32 CFR 170.17(a)(ii)(B).

[13] 32 CFR 170.4.

[14] 32 CFR 170.24(b)(1)(I).

[15] 32 CFR 170.4.

[16] 32 CFR 170.24(b)(1)(ii).

[17] The DoD has estimated that a total of 221,286 companies will be impacted by CMMC,

including 78,085 that will need to be assessed by a third party. See Cybersecurity Maturity Model Certification (CMMC) Program, 89 Fed. Reg. 83092, 83176 (Oct. 15, 2024).

[18] See 32 CFR 170.23(b).

[19] See 32 CFR 170.23(a).

[20] 32 CFR 116 (c)(2) and 32 CFR 117(c)(5).

[21] Id.

[22] The Affirming Official is the senior-level representative from within each defense contractor who is responsible for ensuring the company's compliance with CMMC program requirements and has the authority and responsibility to affirm the company's continuing compliance with security requirements for the company. See 32 CFR 170.4.

[23] 32 CFR 170.22(a).

[24] 32 CFR 170.17(a)(1).

[25]
See https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL1.pdf and https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf.