Alert

November 11, 2021

COZEN O'CONNOR

TIMES THEY KEEP A CHANGIN' — Upcoming Changes to DoD CMMC Program and Cybersecurity Requirements

Lawrence M. Prosen

Member

lprosen@cozen.com
Phone: (202) 304-1449
Fax: (202) 861-1905

Related Practice Areas

- Construction Law
- Government Contracts
- Maritime Regulatory
- Technology, Privacy & Data Security

Industry Sectors

- Maritime

The past few years in the government contracting space has seen significant changes: from the recently passed infrastructure bill and its $1.2 trillion infusion for the modernization of the country's rapidly aging infrastructure, to the heightened need for protections from hackers and ransomware "kidnappers" to the use of cloud computing and storage systems. These are issues that impact not only public contracts but commercial business and the public as a whole. The government continues to work to react to these, and other, areas of concern but often after the fact.

With the more recent discoveries of governmental agencies being hacked repeatedly, as perhaps best exemplified in the Solarwinds situation,[1] the U.S. government has seen a heightened awareness and need for cybersecurity protections. It is in this realm that various federal agencies, with the U.S. Department of Defenses (DoD) taking the lead, have expended significant time and resources to try to catch-up with these cyber-threats; threats that both government and private/commercial entities are experiencing and seeing on a seemingly daily basis.

One of the leading arenas and efforts at heightening protection of the DoD's and its contractors' cyber-infrastructures and information has manifested itself through the CMMC or "Cybersecurity Maturity Model Certification." Under this scheme, the DoD issued a set of rules and frameworks in which Defense Industrial Base (DIB) contractors are required to implement various cybersecurity standards and protections. On November 1, 2021, the DoD issued an Advanced Notice of Proposed Rulemaking, in which it announced that it intends to update its existing, relatively young, CMMC model certification to a CMMC 2.0 structure.[2] While the actual rulemaking has not been issued yet, the subject Advance Notice provides some hints and insights into what is coming.

WHAT IS CMMC?

In laymen's terms, CMMC is a strategy or framework developed by the DoD and its cybersecurity team/agencies (such as DISA) to provide security for both government contracts and sensitive but unclassified information relating to DoD government contracts and other related vehicles and data.

The CMMC program is designed to enhance what has often been basic commercial cyber-protection standards for companies that are within the DIB "universe." Its primary goal is to enhance the protections afforded to sensitive but unclassified information that is shared between the DoD and its contractors and subcontractors. The CMMC program is implemented through contract vehicles (if you have a contract (or often a subcontract) with a DoD entity/agency or sub-agency, you need to generally be CMMC compliant). Simply stated, the CMMC model is intended to enhance and provide further protections for certain types of DoD-related or provided data from those offered by more simple, basic publicly available protects (firewalls, virus software, and the like). This in turn, is expected to provide the DoD with increased assurances that its contractors and subcontractors are not only protecting the DoD-provided data, but are also meeting the DoD's requirements.

As identified by the DoD,[3] the CMMC framework contains three primary features:

- Tiered Model: CMMC requires that those contractor companies entrusted with, and given

access to, certain national security information implement cybersecurity standards at progressively advanced levels. Those levels are dependent upon the type and sensitivity of the data or information provided to them. Additionally, these requirements are flowed down to subcontractors via flowdown provisions to make sure that all parties having access to this data/information have comparable protections in place.

- Assessment Requirement: Through the use of third-party auditors or assessors, the CMMC provides further assurances to the DoD by having third parties verify the proper and timely implementation of the required CMMC cybersecurity standards.
- Implementation Through Contracts: As discussed above, under the current CMMC, and once implemented CMMC 2.0, will require via contract clauses (from the FARs (or Federal Acquisition Regulations found at 48 C.F.R.) and DFARS (Defense FAR Supplement)) that those DoD contractors handling certain sensitive unclassified DoD information be required to achieve a particular CMMC level as a condition of contract award.

CMMC was formally adopted by the DoD in November 2020, when the DoD published an interim rule to the DFARS.[4] That rulemaking implemented the DoD's initial vision for the CMMC program (CMMC 1.0) and outlined the basic features of the framework (tiered models, required assessments, and implementation through contracts). The interim rule became effective on November 30, 2020, establishing a five-year phase-in period — although in reality the implementation was more immediate, as the contract clauses added to contracts presupposed that the contractors already had, or would have in short order, the necessary systems, audit/verification reports, and other obligations to comply if the relevant provisions are contained in the contract in question.

As described in the October 2020 rulemaking, the original intent behind CMMC was to reduce the risk of exposure and theft of intellectual property and sensate information due to malicious hacking and infiltrations. This included the exposure of unclassified information within the supply chain, where, for example contract-related information such as design, formulae, etc. would be provided by the DoD to contractors, and then those contractors would be hacked. In turn, CMMC came out of this concern and tied that framework in with NIST (National Institute for Standards and Technology) SP 800-171 assessments, in which a model and structure for developing and auditing a contractor's cybersecurity were developed.

Starting in March 2021, the DoD initiated a review of its initial effort, asking for public comments and an internal analysis. In November 2021, the DoD announced CMMC 2.0, an updated program structure and requirements was forthcoming. It is designed to achieve the primary goals of the internal review:

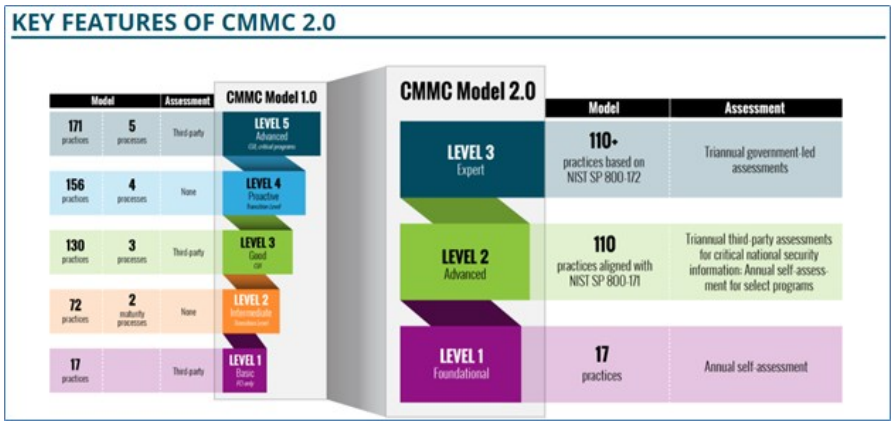
- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber-resilience
- Maintain public trust through high professional and ethical standards.

To achieve these goals, the DoD is eliminating levels 2 and 4, removing CMMC-unique practices and all maturity process from the CMMC, allowing for self-assessments with an annual affirmation by the DIB contractor leadership for CMMC Level 1; bifurcating Level 3 to separate that level between prioritized and non-prioritized acquisitions, the former of which will require third-party, independent assessment and the latter, allow for annual self-assessment and affirmation (nee certification) from the company; further developing CMMC Level 5; developing enforceable and timeframe-specific plans of action and milestones; and also having a waiver process that is time-based and selective if it were needed.

The date for the formal rulemaking is still pending.

THE CHANGES

As described in brief detail above, CMMC 2.0 is described in the Advance Rulemaking Notice as making efforts to streamline the process.



Courtesy of https://www.acq.osd.mil/cmmc/about-us.html

POTENTIAL PROBLEMS

CMMC has been in place since November 30, 2020,[5] however, there are many contractors and subcontractors who do not know of, and are not compliant with, CMMC standards and obligations. Likewise, it bears noting that the same can be said of those that use cloud services and have clauses such as DFARS 252.239-7010 “Cloud Computing Services” and DFARS 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting” in their contracts. These provisions mandate the safe handling of certain data (depending upon the type of clause, things such as Covered Defense Information). To accomplish this, covered contractors must meet the requirements of various government-produced and recognized cybersecurity standards, such as NIST SP 800-171, which provides a listing of over 100 cybersecurity protections and requirements. These provisions, coupled with the more recent CMMC provisions at DFARS 252.204-7021 “Cybersecurity Maturity Model Certification Requirements,”[6] is how the DoD has developed and instituted the flowdown and integration into contracts of these CMMC requirements.

While not necessarily implicated in all contracts, it is a good practice for all DoD contractors and subcontractors to have in place proper and robust cybersecurity systems. Tying the two (CMMC and NIST 800-171) together, has created this framework. However, that framework is not without issues.

While the formal rulemaking and resulting regulations have not been issued yet, the “self-certification” or annual self-affirmation (in whatever format that may take) that is identified in the announcement is problematic and could expose certifying entities/officers to possible False Claims Act (FCA) exposure. Hypothetically, there could be a situation where a contractor (or subcontractor) under a covered contract vehicle that has lower priority and allows self-affirmation were to perform its self-assessment improperly and improperly certify its being in compliance when it is not, the resulting improper certification could open that contractor to civil, and even possibly criminal, FCA exposure/liability. At the present time, the contractor world is in a bit of a “wild west” scenario, where the rules are out there; are in the midst of being revised; and the enforcement of these sometimes vague clauses and requirements without any real substantive law or case law to support this, leaves all such contractors open to exposure. Mitigation of these exposures is best done now, proactively, and not in a reactionary way.

Again, much of this will depend upon the final rulemaking, but for now (and for the past two years) contractors and subcontractors performing contracts with the DoD should be aware of the existence of the CMMC and NIST SP 800-171 requirements and the flowdown of those requirements to one’s contract (and subcontract, as applicable). Such flow downs and inclusions have recently been seen by this author, either through the base contract vehicle or though the addition of such provisions via modification, amendment, or exercise of an option on a multi-year contract.

Once the full rulemaking is issued, we expect to publish a more detailed analysis of the requirements set forth therein. For the time being, however, it is worth the effort now to try to verify your current CMMC 1.0 compliance, start your audits/compliance reviews, and “get ahead” of what

will undoubtedly be a further and expanded universe of cybersecurity and information protection requirements to come out of the DoD (and likely other agencies) in the coming months and years.

Lawrence M. Prosen can be reached at lprosen@cozen.com and at 202.304.1449.

---

[1] https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

[2] This notice can be found at: federalregister.gov/d/2021-24160

[3] https://www.acq.osd.mil/cmmc/about-us.html

[4] https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.

[5] https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

[6] *See also*, DFARS 252.204-7019 "Notice of NIST SP 800-171 DoD Assessment Requirements," and DFARS 252.204-7020, "NIST SP 800-171 DoD Assessment Requirements."