THE CMMC HAS ARRIVED: DOD PUBLISHES VERSION 1.0 OF ITS NEW CYBERSECURITY FRAMEWORK AND DISCUSSES PLANNED ROLLOUT

Date: 6 February 2020

U.S. Government Contracts and Public Policy and Law Alert

By: Steven A. McCain, Erica L. Bakies, Amy C. Hoang, Sarah F. Burgart

On January 31, 2020, the Department of Defense ("DoD") publicly released Version 1.0 of the Cybersecurity Maturity Model Certification ("CMMC") framework. The CMMC is a certification framework developed by DoD that measures a defense contractor's ability to safeguard Federal Contract Information ("FCI") and Controlled Unclassified Information ("CUI") handled in the performance of DoD contracts. By FY 2026, CMMC certification will be a requirement for any company doing business with DoD, either as a prime contractor or lower-tier subcontractor. Version 1.0 of the CMMC fills in several gaps from the earlier drafts, which we assess in prior articles.[1] Additionally, the public briefing that accompanied the release of Version 1.0 included new insights into DoD's rollout of the CMMC framework. This alert walks through the CMMC framework, highlights updates from prior drafts, summarizes DoD's proposed rollout, and provides considerations for companies during CMMC implementation.

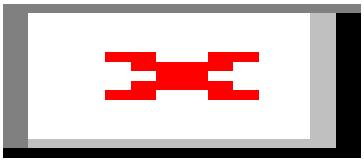
I. KEY TAKEAWAYS

- Version 1.0 fills in several gaps left in the prior draft, namely, discussion and clarification for the Level 4–5 practices. The current version contains slightly fewer practices (171 vs. 173) and processes (5 vs. 9).
- Most significantly, DoD has confirmed that it is planning a phased rollout. DoD will work with agencies to identify "pathfinder programs" that will initially implement CMMC requirements and a complete rollout will take place during FY 2021–25, with all DoD contracts incorporating the requirements by FY 2026.
- DoD is still targeting rulemaking in spring 2020 and expects to release CMMC requirements in ***select*** RFIs in June 2020 and ***select*** RFPs in September 2020.
- Companies that perform non-procurement contracts that are not subject to the DFARS, such as OTAs, may have CMMC requirements implemented as technical requirements.
- DoD officials have suggested that CMMC certifications will remain valid for three years.

II. VERSION 1.0 MODEL OVERVIEW

The CMMC framework includes five levels of certification ranging from Level 1 (basic cyber hygiene) to Level 5 (proactive and advanced cyber practices). Each level consists of practices and processes that a contractor must demonstrate in order to achieve that level of certification.

Version 1.0 of the CMMC model consists of 17 domains (high-level categories of cybersecurity compliance) containing 43 capabilities (achievements to ensure cybersecurity objectives are met within each domain). The capabilities in turn are comprised of 171 practices across the five levels of maturity. Version 1.0 also contains five processes, which refer to an organization's institutionalization of practices. DoD's briefing document for Version 1.0 shows how these domains, capabilities, practices, and processes fit together in the CMMC model:



The five CMMC levels correlate to the following goals:

- Level 1: Safeguard Federal Contract Information (FCI)
- Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3: Protect Controlled Unclassified Information (CUI)
- Levels 4–5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)[2]

The framework consists of both the CMMC model (Appendix A), which lists the practices specific to each level, as well as an appendix that describes in further detail the focus of practices, and the requirements of processes, at each level.

III. WHAT'S NEW IN VERSION 1.0

Version 1.0 closely resembles the prior draft, Version 0.7, in size and content; however, Version 1.0 does contain several notable updates from the prior drafts:

Process Maturity

CMMC Version 1.0 does not include the expected domain-specific processes alluded to in the prior draft. The CMMC framework assigns ratings to contractors based on both their practices (technical activities) as well as their processes (procedures to institutionalize those practices). Version 1.0 contains only five processes (two processes in Level 2 and one process in each of Levels 3–5) compared to the nine processes in Version 0.7. Moreover, Version 1.0 of the model does not describe in detail how each process is tailored to apply to each individual domain, as Version 0.7 had suggested it would.[3] Instead, as in prior drafts, Version 1.0 describes the processes only as generic maturity processes that apply to every domain in the model.[4]

Discussion, Clarification, and Examples for All Levels

Appendix B of CMMC Version 1.0 includes detailed descriptions for each of the 171 practices and five processes across all five levels of the model. Appendix B details: (1) the references from which the practice or process originates; (2) discussion of the practice or process; and (3) clarification of the practice or process, including at least one example of how the practice would be demonstrated within an organization. Version 0.7 provided these descriptions only for the practices associated with Levels 1–3. Version 1.0 now includes detailed descriptions for practices and processes at all levels of the model.

Source Mapping

Appendix E of Version 1.0 is a new “source mapping” resource that provides a detailed table of related practices from other cybersecurity references and frameworks and shows how those practices “map” onto the practices and processes of the CMMC model. While Version 0.7 included a simpler table noting how many practices had been sourced from 48 C.F.R. § 52.204-21, NIST SP 800-171 Rev 1, and Draft NIST SP 800-171B,[5] the new source mapping table in Appendix E details: (1) the specific provisions within references from which a particular CMMC practice or process originates, and (2) source mapping for several other references, including CIS Controls v7.1, CERT Resilience Management Model v1.2, and international cybersecurity frameworks such as the Australian Cyber Security Centre's Essential Eight and the UK National Cyber Security Centre's Cyber Essentials.[6]

Certification Duration

While CMMC Version 1.0 does not address certification duration, DoD's Katie Arrington, Chief Information Security Officer for the Assistant Secretary for Defense Acquisition and a key player in the rollout of CMMC, stated in a press briefing on the morning of the release that a company's certification will be “good” for three years.[7] This suggests that once audited and certified at a certain maturity level, an organization will retain that level of certification for three years before being required to undergo another audit.

IV. PROCEDURAL DEVELOPMENTS

In conjunction with releasing CMMC Version 1.0, DoD provided further insight into how it plans to rollout the framework to its contractors and supply chain.

Phased Rollout Over Five Years

DoD intends to include the new requirements in certain “pathfinder programs,” which will be a limited number of requests for information (“RFIs”) starting in June 2020 and then the corresponding requests for proposals (“RFPs”) in September 2020. While the particular pathfinder RFIs and RFPs are still being determined, DoD indicated that it is targeting 10 RFIs and 10 RFPs, which it estimates would translate to a supply chain of approximately 150 contractors for each awarded contract. DoD also stated that the CMMC requirements for those contracts would be a mix of Levels 1–5, and its initial focus would be on contracts associated with nuclear modernization and missile defense. Although these first steps of the CMMC rollout are expected to take place in the next few months, complete implementation is expected to take five years. As a result of DoD's five-year acquisition cycle (one base year plus four option years), DoD expects that all of its contracts will contain CMMC requirements starting in FY '26, which means that all contractors in DoD's supply chain will need to obtain a CMMC certification in the next five years.

Proposed Rulemaking

Prior to September 2020, DoD intends to undergo rulemaking to implement CMMC into the DFARS, which is what will be included in the relevant RFPs.

CMMC Accreditation Body

With the targeted rollout fast approaching, DoD noted that it was currently drafting a memorandum of understanding between DoD and the newly stood-up Accreditation Body ("AB"), which consists of 13 members from industry. The AB is responsible for training and certifying the third-party assessment organizations ("C-3PAOs"), which will conduct a cybersecurity assessment of DoD contractors. DoD expects the AB to set up a "marketplace" of C-3PAOs on its website in March or early April. Companies can use the marketplace to obtain information on the various C-3PAOs and schedule an assessment for a needed certification level. DoD expects this to be sufficient time to allow companies to obtain the relevant certification by the time of contract award for the pathfinder programs.

CMMC Training

As part of its implementation strategy, DoD is focused on providing resources and ensuring that companies, especially small businesses, will have the ability and time needed to comply with CMMC. To accompany the inclusion of the CMMC requirements in RFIs, DoD is working with the Defense Acquisition University to create and publish a CMMC training in June 2020. DoD confirmed that subcontractors will ***not*** necessarily need to obtain the same level of certification as a prime contractor, such as when the subcontractor's role would not include receipt of CUI. For subcontractor roles that do involve CUI, DoD proposed having small businesses work inside a secure government environment or a prime contractor's environment, instead of having them expend the resources to establish their own infrastructure.

CMMC Requirements for OTAs

Companies that are not typically subject to DFARS requirements are not necessarily off the hook if they perform work for DoD. For nontraditional contracting vehicles, such as Other Transaction Authority ("OTA") agreements and some Small Business Innovation Research/Small Business Technology Transfer agreements, DoD is working with contracting agencies to implement CMMC as a technical requirement. DoD's expectation is that a slow, deliberate CMMC rollout will allow companies to learn, understand, and fulfill their obligations.

V. PREPARING FOR CMMC IMPLEMENTATION

DoD's phased rollout gives industry a bit of a reprieve; however, all DoD contractors and subcontractors must still begin preparations for the CMMC rollout. DoD intends to implement the CMMC requirements using a mix of Levels 1–5. Accordingly, contractors at every level within the CMMC framework need to start preparing for implementation.

Compliance Considerations

Assessing cybersecurity practices at the various CMMC levels is the obvious first step, but companies should also assess their written policies and procedures in order to comply with the CMMC process requirements. Starting at Level 2, companies must have written policies for each of the 17 domains "to establish organizational expectations for planning and performing the activity, and communicate those expectations to the organization,"[8] as well as documented procedures for how they will accomplish Level 1 and 2 practices. At Level 3, the CMMC requires contractors to document a full plan to achieve the objectives in each domain. Higher levels

require documented systems for tracking performance of these procedures and for implementing them across all applicable organizational units.

Public Policy Considerations

Alarm bells have been ringing for the past two years over government cyber vulnerabilities especially in the vast defense industrial base supply chain. The new CMMC requirements have raised deep concerns among industry over the burden and costs compliance could place on small and mid-sized defense contractors in particular.

Federal cybersecurity policy is rapidly evolving, and DoD is pushing for rapid adoption of new certification levels. Industry needs to monitor this changing regulatory landscape and should help develop policy that directly impacts their bottom line, advocating with Congress and the federal agencies to ensure our national security objectives are met and our defense industrial base remains strong. Contractors should consider how they will develop and execute a federal strategy to avoid policy pitfalls and leverage opportunities by engaging with government officials in support of effective CMMC implementation.

VI. CONCLUSION

Release of CMMC Version 1.0 is a major milestone for DoD, but the next year will bring many other CMMC developments. We will continue to monitor the CMMC rollout as DoD releases additional details on its new plan for phased implementation.

---

[1] Amy Conant Hoang, Erica Bakies, and Sarah Burgart, "DOD Clarifies Contractor Cybersecurity Process—Again," *Government Contracts Law360* (December 18, 2019); Amy Conant Hoang and Sarah Burgart, "DOD Clarifies Contractor Cybersecurity Certification Process," *Government Contracts Law360* (November 14, 2019).

[2] CMMC Version 1.0, Jan. 31, 2020, at 4.

[3] *See* CMMC Version 0.7, Dec. 6, 2019, at 7 ("CMMC Version 1.0 will include tailored maturity processes for each domain.")

[4] *See* CMMC Version 1.0, Appendix A at A-2 (listing maturity processes that generically apply to each domain with descriptions such as "Establish a policy that includes [DOMAIN NAME]" and "Review and measure [DOMAIN NAME] activities for effectiveness").

[5] CMMC Version 0.7 at 9.

[6] *See* CMMC Version 1.0, Appendix E at E-1.

[7] *Press Briefing by Under Secretary of Defense for Acquisition & Sustainment Ellen M. Lord, Assistant Secretary of Defense for Acquisition Kevin Fahey, and Chief Information Security Officer for Acquisition Katie Arrington*, Transcript, U.S. Department of Defense (Jan. 31, 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/.

[8] CMMC Version 1.0, Appendix B at B-2.

