SQUIRE PATTON BOGGS

Recently-Released Cybersecurity Verification Mandate Creates Uncertainty for Department of Defense Suppliers

Protection of the Defense Industrial Base (DIB) from the growing panoply of cybersecurity threats has been a consistent point of emphasis for senior Department of Defense (DOD) officials during the Trump Administration. The DOD took a significant step toward addressing that concern on January 31, 2020 with the release of Version 1.0 of the Cybersecurity Maturity Model Certification (CMMC).

The CMMC represents a marked departure from prior DOD cybersecurity compliance mandates. The current DOD cybersecurity requirements, set forth in Section 252.204-7012 of Title 48 (DOD Federal Acquisition Supplement or "DFARS"), permit contractors and subcontractors to self-certify compliance with measures intended to safeguard Controlled Unclassified Information (CUI) generated, accessed, or stored on their IT systems.[1] The release of the CMMC shows that, from the DOD perspective, the existing cybersecurity regulations are considered insufficient.

As currently conceived, the CMMC will require each of the estimated 300,000 contractors and subcontractors in the DIB to achieve a cybersecurity certification by a third party no later than 2026. The CMMC therefore represents a material and potentially costly increase in the sophistication and scale of DOD cybersecurity compliance requirements, and will likely create significant challenges for the DIB in coming years. But those costs are unlikely to deter DOD from moving forward. In her comments at the press conference that accompanied the release of Version 1.0, Under Secretary of Defense for Acquisition and Sustainment Ellen Lord identified the CMMC as a "critical element" of the DOD's "overall cybersecurity implementation."[2]

In this alert, we highlight the key features of the CMMC, identify critical issues that DOD has yet to clarify, and discuss the challenges that the CMMC may create for contractors, subcontractors, and other companies competing for DOD business.

Highlights of the CMMC

Version 1.0 of the CMMC is a broad model framework for improving DIB cybersecurity. It features five levels of certification, beginning with Level 1 (basic cyber practices) and reaching Level 5 (proactive and advanced cyber practices). Each level of certification requires the contractor to demonstrate best practices and processes drawn from the prevailing control standards for cybersecurity, including NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, and AIA NAS9933.[3]

The CMMC is a maturity model, meaning that vendors may progress as they improve their ability to protect Federal Contract Information (FCI) and CUI.[4] Levels 1 and 2 focus on the protection of FCI, while Level 3 is the threshold for contractors possessing CUI. Levels 4 and 5 focus on the protection of CUI and the reduction in risk from intrusion by Advanced Persistent Threats (APTs). DOD anticipates that CMMC certifications will last for three years, and will be valid across service branches.

The CMMC is broken down into seventeen cybersecurity domains, mapped across the five certification levels. Each domain is associated with one or more of forty-three separate CMMC capabilities. These capabilities are in turn associated with at least one or more of one hundred and seventy-one separate CMMC practices. To achieve Level 1 certification under Version 1.0, a contractor will be required to demonstrate seventeen practices, across six domains. By contrast, certification under Level 5 will require demonstration of all one hundred and seventy-one practices, across each of the seventeen domains. The appendices released along with the CMMC provide detailed descriptions of each domain, capability, and practice.

The Under-Secretary of Defense for Acquisition and Sustainment Ellen Lord, in her comments at the release of Version 1.0, described the DOD implementation timeline as "crawl, walk, run"[5], and suggested that a phased roll-out would permit the DIB to gradually adapt to the heightened standards. However, the DOD has firmly identified 2026 as the date when all DOD contracts will include a CMMC certification requirement. That process may begin as early as this year; the DOD currently anticipates issuing ten Requests for Information (RFIs) and ten Requests for Proposal (RFPs) that require CMMC certification as early as October.[6] DOD anticipates that these RFIs and RFPs will encompass up to one hundred and fifty contractors and subcontractors, and require certifications ranging from Level 1 to Level 4.[7]

---

1 Controlled Unclassified Information is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, that does not meet the standards for National Security Classification under Executive Order 12958, as amended. *See* George W. Bush, Memorandum for the Heads of Executive Departments and Agencies, Designation of Sharing of Controlled Unclassified Information (CUI), May 7, 2008; also see Exec. Order 13556, 75 FR 67675 (2010).

2 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 ("Press Briefing", Jan. 31, 2020, *available at* https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/

3 See https://www.acq.osd.mil/cmmc/faq.html

4 Federal Contract Information is information provided by or generated for the Government under contract not intended for public release. *See* 48 C.F.R. § 52.204-21(a).

5 *See* Press Briefing.

6 *Id.*

7 *Id.*

Complicating this process is the absence, at this time, of a Memorandum of Understanding (MOU) between the DOD and the recently created Accreditation Body that will accredit contractors for CMMC compliance. Until the MOU is finalized, contractors are unable to pursue CMMC certification.

Analysis and Key Takeaways

The critical takeaway from the CMMC announcement is that change is coming for contractors, and coming sooner rather than later. But the scale and cost of that change is clouded by uncertainty. For example, the DOD has emphasized repeatedly that the CMMC is a flexible blueprint for effective cybersecurity that will not impose significant compliance or audit costs on smaller contractors and subcontractors. The accuracy of that assessment remains to be seen. At a minimum, the CMMC will require prime contractors to thoroughly assess their existing cybersecurity infrastructure to ensure CMMC compliance. Contractors that routinely work with CUI can anticipate heightened scrutiny of their procedures for controlling access, training employees, securing information, responding to incidents, and assessing the risk of APT intrusion.

It also remains to be seen whether the CMMC will deter commercial companies and start-ups from participating in DOD contracts. In recent years, the service branches have worked diligently to expand their relationships with the smaller, technology-focused companies that often operate on the leading edge of information science. The Air Force has been particularly aggressive in this arena, using Other Transactional Authority (OTA) contracts to rapidly on-board commercial companies and entrepreneurs possessing technology that may prove to have useful military application. Many of these companies had no prior relationship with DOD, and the streamlined OTA process has proven attractive to companies otherwise unwilling or unable to comply with burdensome acquisition requirements. But, the DOD has indicated that CMMC requirements will ultimately be incorporated into OTA contracts, raising the specter of increased cybersecurity compliance costs for small, commercially-focused companies that may be unable to readily fund the necessary upgrades.[8]

Another area requiring further clarification is the impact on suppliers that operate further down the DOD supply chain. If the DOD requires these downstream suppliers to achieve the same CMMC certification as the prime contractor, that could significantly increase the cost of critical components and drive away potential suppliers, particularly smaller organizations that lack a robust compliance function. In her press briefing, Under-Secretary Lord noted that US adversaries often target the "most vulnerable link, which is usually six, seven, eight levels down in the supply chain."[9] It is therefore almost certain that DOD will require prime contractors to ensure CMMC compliance across their supply chain; the question is how onerous these requirements will be.

The certification and audit process also lacks clarity. DOD has yet to provide details on the certification timeline, publish procedures for contesting certification determinations, or identify a workable approach to certifying more than 300,000 companies in less than six years. The recently-formed Accreditation Body only recently launched its website[10], and the information provided does not address these significant questions. It is also unclear whether contractors will be required to conduct annual cybersecurity audits after achieving certification.

Finally, it remains unclear whether CMMC certification will provide any safe harbor for data breaches or intrusions, or any insulation from claims arising under the False Claims Act. The phased rollout of CMMC certification does give contractors a brief respite, but companies that do extensive work with the DOD must begin planning for CMMC certification immediately. Contractors should consider in advance whether to conduct their pre-certification activities under a viable claim of attorney-client privilege and work-product protection. Working with counsel to facilitate pre-certification due diligence may shield privileged documents and communications from discovery in future investigations and litigation.

Contacts

Jack Deschauer
Partner
T +1 202 457 6338
E jack.deschauer@squirepb.com

Pablo Carrillo
Of Counsel
T +1 202 457 6415
E pablo.carrillo@squirepb.com

Karen Harbaugh
Partner
T +1 202 457 6485
E karen.harbaugh@squirepb.com

[8] *Id.*
[9] *Id.*
[10] *See* https://www.cmmcab.org