PUBLICATION

DoD Issues Cybersecurity Maturity Model Certification v1.0 (CMMC)

Authors: Alisa L. Chestler
February 07, 2020

Cybersecurity attacks represent a real threat to our national security and the defense industrial base. To combat these threats, the Department of Defense (DoD) recently released Cybersecurity Maturity Model Certification v1.0 (CMMC). CMMC is a conspicuous change in how cybersecurity will be viewed in the performance of DoD government contracts. Cybersecurity will no longer be viewed primarily as an element of contract performance. Rather, once CMMC is fully implemented, third-party certified and mature cybersecurity practices and processes will be foundational in contracting with DoD – without the appropriate CMMC certification, contractors will not be considered for contract awards. CMMC certification will represent contractors' ticket to get into the game. Without that ticket, contractors will not have a chance to compete for and win DoD contracts.

CMMC is a maturity model comprised of five levels of maturity across both cybersecurity practices and cybersecurity processes. In total there are 171 practices and five processes across the five levels of maturity. The CMMC practices and processes are organized into 17 capability domains:

- Access Control
- Asset Management
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Recovery
- Risk Management
- Security Assessment
- Situational Awareness
- Systems and Communications Protection
- System and Information Integrity

Level 1 represents the requirements needed for DoD contracts that do not involve controlled unclassified information (CUI). Level 2 represents a transitional step to protect CUI. Level 3 governs DoD contracts involving the protection of CUI. Finally, levels 4 and 5 represent the highest levels of maturity for protecting CUI and reducing the risk of advanced persistent threats.

The CMMC takes full advantage of multiple sources of existing cybersecurity requirements. In pulling together the CMMC, DoD incorporated requirements from a variety of sources. For those contractors who already have systems that comply with FAR Subpart 52.204-21 and applicable NIST standards, becoming CMMC certified should not be a herculean task. However, for small and medium sized businesses, certification could prove

difficult, if not impossible. This will provide opportunities for large businesses to mentor, partner with or even acquire small and medium sized businesses. Improving the cybersecurity posture of small and medium sized businesses is critical because our security is only as strong as the weakest link in the acquisition chain. To address some of the concerns associated with less cybersecurity mature contractors, DoD has made it clear that not all procurements are equal and there will be flexibility to assign subcontracts a maturity level lower than that of the prime. For example, if a prime contract is at CMMC Level 3, and a particular subcontract does not involve CUI, that subcontract could be issued at CMMC Level 1.

Another significant change associated with CMMC is the fact that it is a third-party certification system. Currently, DoD contractors self-certify their compliance under the applicable Defense Federal Acquisition Regulation Supplement (DFARS) clauses that primarily rely on the NIST requirements. As we noted in an alert this summer, such self-certifications can lead to potential False Claims Act (FCA) liability. Additionally, contractors have struggled with certifying compliance when the NIST requirements are extensive and therefore can lead to more than one interpretation.

The move to a third-party certification is intended to reduce the confusion with determining compliance and may reduce the risk of FCA liability associated with self-certifications of compliance with applicable cybersecurity requirements, but it does nothing to impact performance risks associated with cybersecurity. It also adds a significant new cost to businesses. As cybersecurity performance and maintaining CMMC certification will be foundational to even obtain DoD contracts, performance risks are heightened. Although it is too early to predict how DoD would react to a significant cybersecurity event or loss of CMMC certification, contract termination would seem to be a more likely result.

Obtaining CMMC certification will only be the beginning. Contractors will have to be continually improving their cybersecurity capabilities and vigilance in response to new and increasing threats in order to ensure their actual performance is strong and they maintain their CMMC certification at the desired maturity level.

In making the announcement, DoD officials made it clear their intent is to implement CMMC in a "crawl, walk, run" sequence. They intend to: (1) issue a new DFARS clause this spring, (2) include the CMMC requirements in approximately ten RFIs this summer, and (3) include the CMMC requirements in approximately ten RFPs this fall. DoD does not intend to modify any existing contracts to include the CMMC requirements. It is anticipated that CMMC will be fully implemented in about five to six years as existing contracts end and are replaced by newly competed contracts containing CMMC requirements. Since government contractors pursuing DoD work will begin seeing these requirements in RFPs later this year, they need to start the process of becoming CMMC certified now.

Companies interested in pursuing DoD contracts should contact the authors, another member of the Baker Donelson Government Contracts Team, or their existing Baker Donelson attorney. In addition, Baker Donelson's Data Protection, Privacy, and Cybersecurity Team routinely assists organizations with privacy and cybersecurity diligence and risk assessments.