Cooley

DoD to Require Contractors to Be Cyber-Certified by Fall 2020

February 28, 2020

On January 31, 2020, the Department of Defense released Version 1.0 of its Cybersecurity Maturity Model Certification (available here) for defense contractors. The model is intended to incorporate and build upon existing cybersecurity frameworks and requirements and is organized into five incremental levels of cybersecurity processes and practices maturity. The lower and intermediate levels (i.e., levels 1-3) cover certifications regarding basic safeguarding of federal contractor information to good cyber hygiene practices with respect to the protection of controlled unclassified information. Levels 4 and 5 reflect advanced cybersecurity practices that not only protect CUI, but also reduce the risk of advanced persistent threats.

The CMMC framework contemplates a certification requirement to have a third-party auditor verify that a contractor has implemented the processes and practices associated with a particular cybersecurity maturity level. CMMC requirements are expected to be noted in requests for information concerning government procurements beginning in spring 2020, after which implementing language will be added to the Defense Federal Acquisition Regulation Supplement by summer 2020. New "go/no go" requirements in requests for proposals are expected by fall 2020. Here is what every defense contractor needs to know to prepare for the changes.

Background: The current cybersecurity clauses and frameworks

Currently, federal contract information, which is information provided by or generated for the government under a federal contract and not intended for public release, is protected pursuant to FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. Such basic safeguarding practices require a contractor to implement certain minimum security controls, such as limiting system access to authorized users, verifying and limiting connections to external systems and escorting visitors and maintaining audit logs of physical access.

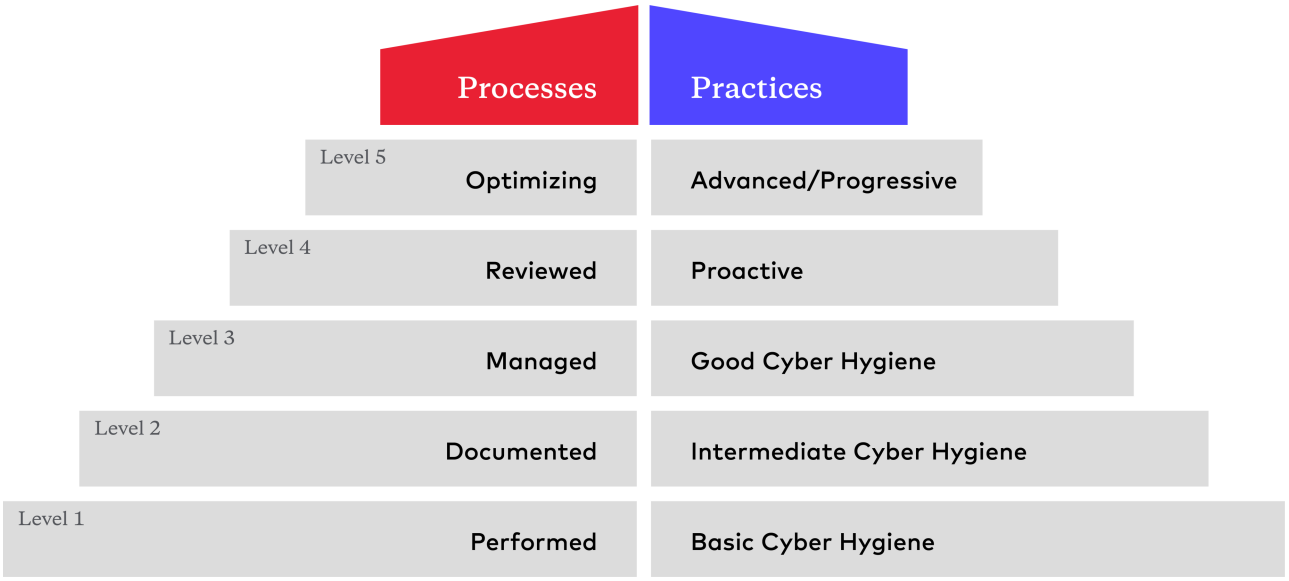
In 2016, DoD issued DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requiring contractors handling CUI (information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations and government-wide policies, but is not classified) to maintain security practices consistent with National Institute of Standards and Technology Special Publication 800-171. Contractors must also report cyber incidents through a specified DoD portal within 72 hours. We summarized the requirements in a client alert (available here).

CMMC builds upon these existing frameworks

The new CMMC will be implemented in the DFARS as an update to DFARS 252.204-7012 and builds upon the existing FAR and DFARS clauses and NIST frameworks. Specifically, CMMC is designed to categorize contractors into five tiers of relative maturity in terms of their cybersecurity processes and practices. Level 1 indicates a contractor has basic cyber hygiene and can safeguard FCI in conformance with FAR 52.204-21. Level 3 indicates a contractor has good cyber hygiene and is capable of protecting CUI in compliance with NIST SP 800-171 pursuant to the existing DFARS 252.204-7012.

More advanced practices will be required to attain a level 4 and 5 certification and will be reserved for contractors that are not only

protecting CUI, but also reducing the risk of ATPs. At these levels, CMMC draws upon NIST's new SP 800-171B's enhanced cybersecurity requirements, which are intended for critical programs and high-value assets. The following graphic illustrates the progression through the five levels, with the status of the contractor's processes indicated in red and its practices in blue (adopted from Figure 2 of CMMC Version 1.0):



In another major change, unlike under the existing DFARS 252.204-7012 regime, CMMC will not permit contractors to self-certify their compliance. Instead, CMMC audits and accreditation will be handled by third-party vendors overseen by a nonprofit accreditation body established by DoD in early 2020.

Audits, certifications and RFP requirements

The task of CMMC accreditation will fall to third-party accreditation vendors, called "CMMC Third Party Assessment Organizations" (C3PAOs). These auditors will begin training in the spring of 2020, and CMMC training is expected to be available online on the Defense Acquisition University website. Around the same time, DoD expects to begin including CMMC requirements in RFIs. DFARS implementing language is anticipated by the summer, in which case we expect such requirements to be included in RFPs as a go/no go factor by the fall.

Significantly, contractors that fail to meet the CMMC level applicable to a solicitation will be ineligible for contract award. The requirements will flow through the entire supply chain, although subcontractors may be permitted to be certified at a lower CMMC level than prime contractors, depending on the scope and nature of the subcontractor's intended work. Contractors should track costs of their certifications, which are expected to be allowable in cost reimbursement contracts.

Full implementation of CMMC is expected to take several years because it will not apply to contractors retroactively – DoD has suggested it may be 2026 before CMMC is incorporated into all DoD contracts as many recently issued contracts will come up for renewal or recompetition. Going forward, the CMMC model will be updated at least annually to keep up with changing threat environments and technological capabilities.

While CMMC contains some significant changes for contractors, such as the third-party audit process, the fact that it builds upon existing frameworks and requirements should make implementation less burdensome than if the framework was created from whole cloth. Regardless of how individual contractors view the CMMC compliance burden, cybersecurity compliance generally is

increasingly a focus of enforcement in federal contracting, as evidenced by two cybersecurity False Claims Act cases last year. *See U.S. v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 39 1240 (E.D. Cal. 2019) (denying a motion to dismiss an FCA claim alleging defendants falsely certified compliance with cybersecurity requirements); *U.S. ex rel. Glenn v. Cisco Systems, Inc.*, No. 1:11-cv-400-RJA (W.D.N.Y.) (involving an $8.6 million settlement resolving FCA allegations that the defendant's product did not comply with federal cybersecurity requirements).

Contractors that begin planning for the forthcoming changes now will be prepared for the CMMC requirements in solicitations later this year. For help, contact Cooley's government contracts team: Erin Estevez, Pablo Nichols and Chris Kimball.

Key Contacts

Christopher Kimball Washington, DC	ckimball@cooley.com +1 202 842 7892