Updates
February 03, 2020

DoD Releases New Cybersecurity Verification Standard

The U.S. Department of Defense's (DoD) new cybersecurity verification regime is moving into a new phase, with major implications for contractors.

On January 31, 2020, DoD released version 1.0 of its Cybersecurity Maturity Model Certification (CMMC). Under CMMC, each of roughly 300,000 defense suppliers will need to be certified under one of five CMMC levels in order to be eligible for a defense contract.

DoD plans on rolling out CMMC in a phased approach, acknowledging the significant impact that the model will have on industry, including small and medium-sized businesses. During a news conference to announce the release of CMMC Version 1, Ellen M. Lord, undersecretary of defense for acquisition and sustainment, described the rollout approach as "crawl, walk, run."

This update provides an overview of version 1 of CMMC and some of the significant issues that contractors should be aware of as the implementation process continues.

Implementation Timeline—Many Steps Remain

CMMC reflects DoD's view that protecting the defense supply chain against malicious cyber activity and intellectual property theft is an urgent matter of economic and national security. It also demonstrates DoD's conclusion that the existing regulatory framework under the Federal Acquisition Regulation (FAR) and Defense FAR Supplement (DFARS), which has to date relied on companies self-attesting compliance, does not go far enough.

DoD plans to include CMMC requirements in select requests for information and solicitations in June and September 2020, respectively. According to Katie Arrington, DoD's chief information security officer for acquisition, DoD has identified 10 select "pathfinder" contracts involving 150 contractors for those initial requests. She said CMMC will not be inserted into existing contracts but rather introduced gradually over a five-year process as contracts are re-competed.

The following are several remaining steps that could affect the timeline—and substance—of the new standard:

- **Rulemaking Process.** DoD has initiated a rulemaking process to revise its cybersecurity requirements in the DFARS. DoD aims to complete the rulemaking process by September 2020, which is an ambitious timeline. The prospect of regulatory changes after the opportunity for public comment introduces a significant element of uncertainty as companies evaluate what CMMC means for them. It is unclear, for example, to what extent existing cybersecurity requirements in DFARS 252.204-7012 (*Safeguarding Covered Defense Information and Cyber Incident Reporting*) will be changed.
- **Training and Accreditation of Auditors.** Under CMMC, an independent auditor known as a Third-Party Assessment Organization, or C3PAO, will perform an audit of a company's systems and determine eligibility for a given CMMC level. Those auditors still need to be selected. The newly established CMMC Accreditation Body, a nonprofit organization responsible for managing CMMC, will need to train and accredit auditors.

- **CMMC Accreditation Body.** DoD needs to complete a Memorandum of Understanding with the CMMC Accreditation Body. According to Ms. Lord, this document will outline the roles, responsibilities, and rules for accreditation. She said one focus is preventing conflicts of interest by prohibiting an auditor from reviewing its own company.

Highlights of Version 1

Version 1.0 of CMMC follows DoD's release of several initial versions of the model late last year. Each of those versions was modified based on comments and input from industry and others.

Version 1.0 of the model has five levels, ranging from basic hygiene (Level 1) to sophisticated controls intended to combat advanced persistent threats (Levels 4 and 5). The model consists of maturity processes and 171 cybersecurity best practices borrowed from several sources. A majority of those practices (110 of the 171) originate from FAR 52.204-21 (*Basic Safeguarding of Covered Contract Information Systems*) and DFARS 252.204-7012. The latter clause requires defense contractors to implement certain controls in National Institute for Standards and Technology (NIST) Standard Protocol (SP) 800-171. The model organizes processes and practices into a set of 17 domains and maps them across the five CMMC levels.

CMMC Version 1.0 includes 336 pages of appendices. Appendix B provides a detailed discussion of each process and practice in the CMMC model. Appendix E provides a table that maps each CMMC practice against sources in other frameworks to enable organizations to identify which CMMC practices correspond to ones they may already be using.

Level 3 will apply to contractors that possess Controlled Unclassified Information (CUI), which is broadly defined as any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls. At Level 3, a contractor will be required to comply with 130 practices, including all 110 practices from the NIST SP 800-171 rev. 1. At CMMC Levels 4 and 5, contractors must comply with 156 and 171 practices, respectively, and thus be able to protect CUI and reduce the risk of advanced persistent threats.

Implementation Issues

CMMC raises numerous challenges and questions for contractors doing business with DoD.

- **Flow-down Issues.** DoD has made clear that prime contractors will be required to flow down the appropriate CMMC requirements to subcontractors. It remains uncertain what procedures will be used to determine the appropriate CMMC level for subcontractors at various tiers. Ms. Arrington clarified during the news conference that the CMMC level for a prime contractor does not necessarily apply to each of its subcontractors. Thus, all subcontractors will need to be certified, but not necessarily at the same level.
- **Assessment Levels.** A DoD procuring agency will determine the appropriate CMMC level for a given acquisition. What criteria the agency will use to decide which level to use for a given procurement remains to be seen.
- **Auditing Issues.** Various questions remain as to how the CMMC Accreditation Body will operate, and how it will monitor and maintain quality and uniformity among auditors. Another important issue for industry is the role of supply chain-related audits performed by other agencies, such as the Defense Contract Management Agency (DCMA).
- **Small Business Impact.** Ms. Lord stated during the news conference that one of her "biggest concerns" is implementing CMMC for small and medium businesses. According to Ms. Lord, DoD is considering ideas proposed by prime contractors to "more cost effectively" accredit such businesses, including developing "a

number of different groups to streamline the certification process." DoD has indicated that cybersecurity costs will be allowable, indirect costs under government contracts. But it remains unclear how much companies will have to spend to obtain—and maintain—the necessary certifications and whether and how compliance costs will be recoverable.

- **Source Selection**. The CMMC level for a given procurement will be specified in an agency's Request for Information or Request for Proposal. CMMC will be a "Go/No Go" criteria in the source selection process. Ms. Arrington clarified that an offeror will need the proper certification at the time of contract award. She noted that CMMC will be included as a technical requirement in Other Transaction (OT) agreements, which the DoD has been increasingly using as an alternative to traditional contract vehicles.

Authors

Richard W. Oehler

Partner
ROehler@perkinscoie.com 206.359.8419

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Explore more in

Government Contracts Privacy & Security

Related insights

Update

'Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers

Update

Employers and Immigration Under Trump: What You Need To Know