Cybersecurity Maturity Model Certification (CMMC)
(February 2021)

By David Drabkin

In 2019 the Department of Defense (DoD) embarked on an effort to improve the cybersecurity of its supplier base in order to reduce the threat that potential adversaries and nonstate actors pose to DoD specifically and the U.S. economy generally**.** The Office of the Secretary of Defense (OSD) announced at the inception of this undertaking that security should not be traded for cost, schedule and performance. CMMC is focused on enhancing the security of controlled unclassified information (CUI) in the supply chain. **https://www.acq.osd.mil/cmmc/index.html.**

The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.

- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- Authorized and accredited CMMC Third Party Assessment Organizations (C3PAOs) will conduct assessments and issue CMMC certificates to Defense Industrial Base (DIB) companies at the appropriate level.

[Editor’s note: The CMMC v. 1.02 (March 2020) is available at https://www.acq.osd.mil/cmmc/draft.html]

The CMMC is based on a standard upon which contractors are evaluated and assigned a certification. There are five levels of CMMC certification, levels 1 – 5. DoD originally planned on a gradual roll out of the CMMC program with requests for information (RFIs) beginning in May 2020 and requests for proposals (RFPs) beginning in Sep 2020, which will identify the rating a contractor must have in order to be eligible to receive award of the resulting contract. For a variety of reasons the roll out of the program was slowed. An Interim Rule, Defense Federal Acquisition Regulations Supplement (DFARS) rule, DFARS Case 2019-D014, Strategic Assessment and Cybersecurity Certification Requirements, https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf, was issued on September 29, 2020 with an effective date of November 30, 2021. Comments on the Interim Rule were due to the government on November 30, 2021, a Final Rule has not been issued as of this writing.

The standard, now V 1.02, was developed by Carnegie Mellon University and John Hopkins University under contract. Comments were invited from the public during the development process. The standards are based in part on the National Institute of Standards and Technology (NIST) SP 800-17, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations now rev. 2, dated January 28, 2021, https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final. The levels are divided into practices and processes.

Certifications will be awarded to companies by private sector organizations, certified third-party assessment organizations (C3PAOs), applying the CMMC model to the company's information technology "hygiene." Certifications will be renewed periodically. The C3PAOs in turn will be accredited by a private sector non-profit organization, the CMMC Accreditation Board (AB), https://www.cmmcab.org/.

DoD's decision to create this process is not driven by statute. There are lots of questions to think about. Here are a few to think about.

- Is this an overly restrictive requirement? Could the gov't achieve its needs by a less restrictive program? What's the impact on competition? If you wanted to protest the requirement for CMMC certification, which forum would you choose?

- Does this requirement violate the WTO Government Procurement Agreement or bilateral or regional agreements, including reciprocal defense procurement agreements? Can foreign companies obtain certifications?

- Can you be NIST 800-171 compliant if you are physically located or have affiliates or subsidiaries or suppliers outside the continental United States (OCONUS)?

- What is the impact of Section 889(a)(1)(A) & (B) of the FY19 NDAA on a firm's ability to be CMMC compliant? How does use of a commercial internet service providers, e-mail providers, or cloud providers impact a firm's ability to be certified?