GT GreenbergTraurig

Alert | Government Contracts

October 2019

New Cybersecurity Certification Requirements for Government Contractors

The Office of the Under Secretary of Defense for Acquisition and Sustainment has been working since March 2019 in a collaborative effort with Johns Hopkins University Applied Physics Laboratory, Carnegie Mellon University Software Engineering Institute, Defense Industrial Base Sector Coordinating Council (DIB SCC), the Office of Small Business Programs, as well as many other organizations to develop the Cybersecurity Maturity Model Certification (CMMC) requirement for government contractors. The CMMC effort has had a great deal of support from industry associations such as the National Defense Industrial Association, the Aerospace Industries Association, and the Professional Services Council in getting CMMC information out to the Department of Defense (DoD) supply chain.

The goal is for CMMC to be a unified cybersecurity standard for all DoD acquisitions, to reduce what is termed the "exfiltration" of Controlled Unclassified Information from the Defense Industrial Base. The current CMMC Schedule is to release CMMC Rev 1.0 in January 2020, followed by the inclusion of CMMC in Requests for Information starting in June 2020 and in Requests for Proposals (RFPs) starting in Fall 2020. The ultimate goal is to require all companies conducting business with DoD to obtain CMMC for both prime contracts and subcontracts.

The CMMC effort builds upon existing regulations and standards including "Safeguarding Covered Defense Information and Cyber Incident Reporting" (Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012) and "Protecting Controlled Unclassified Information in Nonfederal Systems and

Organizations" (National Institute of Standards and Technology (NIST) SP 800-171), by adding a verification component with respect to cybersecurity requirements.

The CMMC will encompass multiple maturity levels that range from basic cybersecurity "hygiene" to highly advanced cybersecurity practices reserved for the most critical systems. We especially note that the intent is to identify the required CMMC level in RFP sections L and M and use it as a "go/no go" evaluation threshold. It is unclear whether an offeror still in the process of obtaining its CMMC at the time it submits its initial offer will be allowed to continue the process up to a certain point or will be immediately excluded from further consideration.

A company seeking to be certified must coordinate directly with an accredited and independent third-party commercial certification organization (no self-certification will be permitted). The company will specify the level of certification requested based on the company's specific business requirements. The company will then be awarded certification at the appropriate CMMC level upon demonstrating the appropriate maturity in capabilities and organization to the satisfaction of the certifying organization. DoD intends to make public the CMMC level achieved by contractors. This will have a critical impact on business opportunities.

As currently designed, the CMMC model framework consists of 18 domains (i.e., Access Control, Asset Management, Audit and Accountability, Awareness and Training, Configuration Management, Cybersecurity Governance, Identification and Authorization, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Recovery, Risk Assessment, Security Assessment, Situational Awareness, System and Communications Protection, and System and Informational Integrity), which will have key sets of capabilities for cybersecurity, based on cybersecurity best practices. The domains each list capabilities that ensure cybersecurity within that domain, and these capabilities in turn are listed and mapped to CMMC Level 1 though Level 5.

Level 1 is the lowest, covering basic cybersecurity and universally accepted common practices that provide limited resistance against data exfiltration and limited resilience against malicious actions. The practices found in Level 1 include compliance with DFARS requirements and the use of anti-virus software. Level 5 covers highly advanced cybersecurity practices, reserved for the most critical systems, requiring the systems to be resilient against the most-advanced threat actors. Examples of Level 5 practices includes deployment of organizational custom protections, real-time asset tracking, device authentication, and context aware access control and step-up authentication. CMMC Levels 4 and 5 are targeted toward a small subset of the DIB sector that supports DOD critical programs and technologies.

DoD will be accepting feedback for the draft CMMC Rev. 0.6 in November 2019.

Authors

This GT Alert was prepared by **Richard L. Moorhouse** and **Józef S. Przygrodzki**. Questions about this information can be directed to:

- Richard L. Moorhouse | +1 703.749.1304 | moorhouser@gtlaw.com
- Józef S. Przygrodzki | +1 703.903.7591 | przygrodzkij@gtlaw.com
- Or your Greenberg Traurig attorney

Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.