Published on *The National Law Review* https://natlawreview.com

DoD's Cybersecurity Maturity Model Certification Is Here: What Your Business Needs to Do to Prepare

Article By:

Peter Baldwin

Jason G. Weiss

On September 1, 2020, Department of Defense (DoD) contractors will be required to comply with the recently released Cybersecurity Maturity Model Certification (CMMC) requirements. The CMMC requirements are designed to ensure that suppliers, contractors and subcontractors working with the DoD's Office of Acquisition and Sustainment have cybersecurity frameworks in place "to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB)." Through the creation of the CMMC, DoD appears to be enhancing the requirements of NIST 800-171, ISO 27001 and other cybersecurity-related frameworks.

The CMMC model delineates five "maturity" levels, with level 1 being the least secure and level 5 being the most secure. Once the CMMC takes effect, DoD will assign all solicitations an appropriate maturity level that bidders must be able to meet if they wish to bid on the solicitation.

Potential bidders also will have to meet 17 "security domains" within each of the five maturity levels of the CMMC. These maturity levels are cumulative, meaning that if a company wants to certify at level 3 under the CMMC requirements, it would also have to comply with all of the requirements of levels 1 and 2. Thus, a winning level 5 bidder could be required to comply with up to 171 different cybersecurity requirements in order to meet CMMC certification guidelines. The level of maturity that a company will need to obtain will be based on the amount of sensitive data, Controlled Unclassified Information (CUI), and unclassified data that requires specific safeguarding that the company works with or plans to work with as a DoD contractor or subcontractor.

One of the most notable aspects of the CMMC requirements is that it they prohibit contractors and subcontractors from "self-certifying" their cybersecurity readiness. Under the CMMC, contractors will need to have an official, independent third-party assessment organization ("C3PAO") conduct a formal certification inspection to ensure that the DoD contractor is in strict compliance with the CMMC requirements. Failure to comply with the requirements of a particular maturity level renders the contractor unable to bid on new DoD solicitations that require the maturity level in question. Although the CMMC guidelines currently do not appear to be retroactive, DoD solicitations will begin referring to CMMC requirements as early as June 1, 2020, and the requirements will become mandatory on September 1, 2020.

Given the impending deadlines, the time for DoD contractors and subcontractors to start preparing to comply with the CMMC requirements is now. Faegre Drinker's team can assist in the preparation process, including, among other things, the C3PAO compliance process. The firm also has prepared an assessment and compliance tool to assist businesses in achieving maturity levels 1 through 5 and in developing the necessary policies, procedures and gap analyses to comply with the CMMC requirements.

National Law Review, Volume X, Number 106