Inside Government Contracts

*Procurement Law and Policy Insights*

FROM COVINGTON & BURLING LLP

COVINGTON

# DoD Announces the Cybersecurity Maturity Model Certification (CMMC) Initiative

*By Susan B. Cassidy, Melinda Lewis and Weiss Nusraty on July 16, 2019*
Posted in Cybersecurity, Defense Industry, Government Contracts Regulatory Compliance

The Department of Defense ("DoD") recently announced the development of the "Cybersecurity Maturity Model Certification" ("CMMC"), a framework aimed at assessing and enhancing the cybersecurity posture of the Defense Industrial Base ("DIB"), particularly as it relates to controlled unclassified information ("CUI") within the supply chain.

The Office of the Under Secretary of Defense for Acquisition and Sustainment has created a **website** that provides additional background on the proposed CMMC, including a list of FAQs and details about a CMMC Listening Tour that is intended to solicit feedback from key DIB stakeholders. DoD is planning to release Version 1.0 the CMMC framework in January 2020 and expects to incorporate CMMC requirements in Requests for Proposals ("RFPs") beginning in June 2020.

The concept of a CMMC framework arose in response to a series of high profile breaches of DoD information. This caused DoD to reevaluate its reliance on the security controls in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 as sufficient to thwart the increasing and evolving threat, especially from nation-state actors. Katie Arrington, Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber, Office of the Under Secretary of Acquisition and Sustainment, is among those leading this effort and addressed DoD's plans for the CMMC at the May 23, 2019 Georgetown Cybersecurity Law Institute.

Key takeaways from the CMMC website include:

- The initial implementation of the CMMC is for DoD only. However, the use of CUI terminology rather than covered defense information ("CDI"), which is used in DFARS 252.204-7012, indicates a potentially broader role for this model beyond DoD.
- All companies conducting business with the DoD, including subcontractors, must be certified.
- The CMMC is expected to combine relevant portions of various cybersecurity standards, such as NIST SP 800-171, NIST SP 800-53, ISO 270001, and ISO 27032, into one unified standard for cybersecurity. Unlike NIST SP 800-171, which measures a contractor's compliance with a specified set of controls, the CMMC will more broadly "measure the maturity of a company's institutionalization of cybersecurity practices and processes."
- The CMMC is expected to designate maturity levels ranging from "Basic Cybersecurity Hygiene" to "Advanced." For a given CMMC level, the associated controls and processes, when implemented, are intended to reduce risk against a specific set of cyber threats. Notably, DoD will assess which CMMC level is appropriate for a particular contract and incorporate that level into Sections L and M of the RFP as a "go/no go" evaluative determination. This assessment of appropriate maturity levels on a procurement basis is akin to the Cyber Security Model that the United Kingdom's Ministry of Defence ("MoD") currently employs for all MoD contracts.
- In general, contractors will be required to be certified by a third-party auditor. The FAQs on the website note that certain "higher level assessments" may be conducted by government assessors, including requiring activity personnel, the Defense Contract Management Agency ("DCMA"), and the Defense Counterintelligence and Security Agency ("DCSA"). The website does not, however, explain what qualifies as a higher level assessment.
- How long a certification will remain in effect is still under consideration. Additionally, certification levels of contractors will be made public, though, details of specific findings will not be publicly accessible.
- A compromise of a contractor's systems will not result in automatic loss of certification. However, depending on the circumstances of the compromise, it appears that DoD intends to authorize program managers to require recertification if they believe necessary. It is unclear whether this obligation will be imposed via contract or regulation and what standard will be used to determine that a recertification is necessary.

- The cost of certification will be considered an allowable, reimbursable cost. The FAQs state that the costs "will not be prohibitive."

**Impact on Contractors**

It is too early to assess the potential impact of the CMMC on contractors. Although details relating to the scope, breadth, and implementation of the CMMC are limited, the framework reflects DoD's first meaningful attempt to impose a broader assessment regime. It is unclear whether implementation of the CMMC will eliminate the need for DCMA to conduct audits to measure compliance with NIST SP 800-171.

DIB stakeholders will have a number of opportunities to provide feedback. The CMMC Listening Tour is expected to include five outreach events throughout July and August 2019, with more expected before the framework is released in January 2020.

---