THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 61, No. 37 **October 9, 2019**

Focus

¶ 293

FEATURE COMMENT: Cybersecurity For Government Contractors: DOD's New Cybersecurity Maturity Model Certification Rapidly Taking Shape

Defense contractors and their lower-tiered subcontractors will face tight deadlines over the next year to comply with the Department of Defense's new and evolving Cybersecurity Maturity Model Certification (CMMC) framework. DOD currently expects to include requirements for CMMC certification in solicitations beginning in fall 2020. Solicitations will require that prime contractors flow down CMMC certification requirements to their lowest-tiered subcontractors, meaning anyone that does business with DOD (not just prime contractors) will need to achieve CMMC certification.

On Sept. 4, 2019, DOD released CMMC Rev 0.4, a "unified cybersecurity standard for DOD acquisitions." The current draft is available at *www.acq.osd.mil/cmmc/draft.html*. The CMMC model is still in development. DOD expects to finalize v1.0 of the CMMC in January 2020. The CMMC, as currently drafted, represents a major shift for DOD supply chain cybersecurity policy. First, compliance with CMMC will be based upon certifications provided by outside monitors rather than through self-attestation. Second, the CMMC will include multiple levels of certification requiring increasingly more stringent cybersecurity policies and practices. Finally, all DOD contractors and lower-tiered subcontractors will be required to achieve CMMC certification, not just those with access to Covered Defense Information (CDI).

Shift from Self-Attestation to Third-Party Verification—Since Dec. 31, 2017, all DOD contractors have been required to meet the Defense Federal Acquisition Regulation Supplement 252.204-7012 requirement to provide "adequate security" for information systems that process, transmit or store CDI. The DFARS clause defines CDI as (1) Controlled Unclassified Information (CUI) provided by DOD to the contractor or "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract"; and (2) technical information with military or space application that is subject to use and dissemination controls. CUI is the umbrella term for unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations and Government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. See EO 13556 "Controlled Unclassified Information," 75 Fed. Reg. 68,675 (Nov. 9, 2010); 32 CFR pt. 2002 "Controlled Unclassified Information." See also Scott A. Schipma, "Cybersecurity for Government Contractors: New Controlled Unclassified Information (CUI) Requirements Slowly Taking Shape" (Oct. 28, 2015), available at *www.lexology.com/library/detail.aspx?g=39920dbf-15cc-494e-b5a4-58088ff38b99*, archived at *perma.cc/6U6V-MYQH* (discussing the regulatory history of cybersecurity requirements for Government contractors with access to CUI).

At a minimum, DFARS 252.204-7012 requires contractors performing work on a DOD contract involving CDI to implement the version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, in effect at the time the contract's solicitation was issued. DOD guidance states that contractors may meet these cybersecurity requirements by self-attesting to compliance with DFARS 252.204-7012 and implementation of NIST SP 800-171. Department of Defense, *Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified*

Information System (Nov. 6, 2018), available at *www.acq.osd.mil/dpap/pdi/cyber/docs/Assess. Compliance and Enhance Protection of Contractor System with Attachments 2011-6-2018.pdf* archived at, *perma.cc/V3NE-3787*.

In contrast to the current self-reporting system, the CMMC framework will require defense contractors to have their information systems certified by outside auditors. DOD will authorize a yet-unnamed nonprofit organization to accredit and oversee CMMC auditors. To prevent conflicts of interest, CMMC auditors will be prohibited from providing services to defense contractors related to achieving CMMC certification. DOD's current timeline suggests auditors will begin granting CMMC certification beginning in June 2020. During a July 17, 2019 Professional Services Council webcast, Katie Arrington, the Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber, stated that DOD expected businesses currently fulfilling healthcare privacy audit roles and others to enter the market in sufficient numbers to meet the expected demand for CMMC auditors.

Establishment of a Tiered, 5-Level Certification Approach—The CMMC will build on existing cybersecurity standards, including the Aerospace Industries Association NAS9933, CERT Resilience Management Model, International Organization for Standardization (ISO) 27001, ISO 27032, NIST SP 800-53, NIST SP 800-171 and certain aspects of NIST SP 800-171B. DOD's goal is to ensure that CMMC certification will satisfy existing cybersecurity standards. Office of the Under Secretary of Defense for Acquisition and Sustainment, *Cybersecurity Maturity Model Certification*, available at *www.acq.osd.mil/cmmc/index.html* (last accessed: Sept. 10, 2019).

Currently, the CMMC framework identifies 18 domains (Asset Management, Cybersecurity Governance, Recovery, Situational Awareness, and the 14 security requirement families identified in NIST SP 800-171). Each domain includes various cybersecurity capabilities and processes. Capabilities and processes are further subdivided into various maturity levels. For example, the "Media Protection Domain" includes the "Protect CUI during personnel actions" capability, which is defined at "Level 1" as "CUI is protected during personnel actions at least in an ad hoc manner," and at "Level 2" as "The organization has a process to ensure CUI is protected during personnel actions." Draft CMMC Rev 0.4, at 35, available at *www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf.*

In contrast to the current, one-size-fits-all approach, the CMMC will include five "maturity levels" of certification ranging from Level 1 (Basic Cyber Hygiene—Performed) to Level 5 (Advanced/Progressive—Optimized). For example, to achieve Level 1 certification, contractors will need to demonstrate compliance with the 15 basic safeguarding requirements and procedures set out in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems; and to achieve Level 3 certification, contractors will need to demonstrate compliance with all NIST SP 800-171 Rev 1 controls. DOD will assess each acquisition (and as appropriate, certain individual requirements) to determine the required level of CMMC certification. This tiered approach is intended to reduce the cybersecurity burden on contractors and suppliers performing low-risk efforts, while at the same time ensuring that DOD has the flexibility to impose more stringent requirements for higher-risk acquisitions. DOD stated that the "goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels." Office of the Under Secretary of Defense for Acquisition and Sustainment, *Cybersecurity Maturity Model Certification*, available at *www.acq.osd.mil/cmmc/index.html* (last accessed: Sept. 10, 2019). This tiered approach, however, introduces uncertainty for contractors as they attempt to anticipate which CMMC level certification DOD might impose on procurements of interest.

Rapid Implementation Required for the Entire Defense Industrial Base—Over seven years elapsed between the issuance of EO 13556, directing agencies to develop and implement CUI policies, and the implementation of DFARS 252.204-7012, requiring contractors to provide adequate security for systems handling CUI and other CDI. By contrast, DOD intends to implement the CMMC following a much more rapid schedule.

Instead of revising the FAR or DFARS, DOD intends to quickly implement the CMMC by including certification requirements in requests for information (RFIs) for procurements beginning in June 2020, and by including go/no-go evaluation factors in all DOD requests for proposals beginning in fall 2020. See *Cybersecurity Maturity Model Certification (CMMC): Draft CMMC Model Rev 0.4 Release & Request for Feed Back* (September 2019), at 4, available at *www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf*, archived at *perma.cc/Z9PT-Y9ND* (CMMC Overview Briefing) (CMMC "[w]ill be included in RFIs starting in June 2020."). For any solicitation including a CMMC certification go/no

go factor, contractors will not be eligible for award unless they demonstrate the appropriate level of CMMC certification. Significantly, the CMMC certification requirement is expected to be a required flow-down to all lower-tiered subcontractors, regardless of whether the subcontractors have access to CDI. Office of the Under Secretary of Defense for Acquisition and Sustainment, *CMMC FAQ's*, available at *www.acq.osd.mil/cmmc/faq.html,* archived at *perma.cc/KN9K-4ZA5* ("Q: I am a subcontractor on a DoD contract. Does my organization need to be certified? A: Yes, all companies doing business with the Department of Defense will need to obtain CMMC.").

DOD is currently conducting public meetings and reviewing feedback on draft CMMC Rev 0.4. DOD expects to solicit additional public feedback on draft CMMC Rev 0.6 in November 2019. In the meantime, DOD has scheduled public meetings to discuss the CMMC with various stakeholders. Current information on the DOD's CMMC Listening Tour is available at *www.acq.osd.mil/cmmc/listening-tour.html*.

Outstanding Questions

- Who will be responsible for administering the CMMC framework? DOD has indicated that it will designate a nonprofit organization to oversee the CMMC certification process. However, DOD has not provided information regarding what entity will take on this role, or to what extent the entity will be subject to DOD oversight and direction.
- How will contractors achieve certification? DOD intends for outside auditors to make certification determinations; however, DOD has not released any guidance regarding how those determinations will be made. How will contractors be expected to demonstrate compliance with the CMMC's requirements for various capabilities and processes? Will each capability and process be weighted equally? Will contractors have the opportunity to appeal adverse CMMC audits?
- How will DOD decide what CMMC certification level is appropriate for particular acquisitions? Will DOD release guidance as part of the CMMC rollout? Is this an area that contractors will have the opportunity to challenge in preaward protests?
- How will contractors pay for CMMC compliance? Through its Listening Tour, DOD has indicated that it plans to make CMMC an allowable cost. However, it is unclear to what extent the Government plans to reimburse contractors for CMMC expenses and how the reimbursement will occur (especially for commercial and other contracts without the opportunity for contractors to charge indirect rates).
- Will the CMMC model eventually apply to non-DOD contracts?

What Steps Should Contractors Consider?

- Contractors should closely monitor the development of the CMMC because of DOD's aggressive implementation timeline. Currently, contractors may be required to achieve CMMC certification to compete for solicitations issued as early as fall 2020;
- Contractors should continue to implement and comply with their NIST SP 800-171 System Security Plans. It is unclear at this stage whether CMMC will simply supplement or replace requirements to meet the NIST SP 800-171 guidelines;
- Contractors should ensure that they are prepared to flow down CMMC certification requirements because DOD has indicated that it expects for the CMMC framework to apply to all DOD suppliers throughout the supply chain. Contractors should begin discussing the CMMC framework with their current subcontractors. Contractors should also consider CMMC certification requirements when negotiating future teaming and subcontractor agreements; and
- As appropriate, contractors should consider providing feedback to DOD through public comments or attendance at one of DOD's Listening Tour events.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Scott A. Schipma *(schipmas@gtlaw.com),* Daniel D. Straus *(strausd@gtlaw.com) and* Danielle K. Muenzfeld *(muenzfeldd@gtlaw.com)* of *Greenberg Traurig, LLP (GT). Scott is a shareholder in GT's Government Contracts & Projects Practice. Daniel and Danielle are associates in GT's Government Contracts & Projects Practice.

