PUBLIC CONTRACTING INSTITUTE

CMMC 2.0: Now What – An Office Hours Q&A

Alex Major
Franklin C. Turner

January 31, 2024

PUBLIC CONTRACTING INSTITUTE

Who Are These People?

- Co-Leaders of the Government Contracts and Global Trade practice at McCarter & English, LLP
- Significant experience handling “bet the company” litigation for multinational corporations to small businesses
- Overseen compliance obligations addressing cybersecurity, SBA requirements, CAS and cost-accounting and the gambit of FAR/DFARS issues
- Handled claims and bid protests valued, in the aggregate, in the tens of billions of dollars

CMMC 2.0 – Coming Now

- Let's avoid the guesses, history, and sales pitches addressing the Cybersecurity Maturity Model Certification - key decision makers (and the people they may task) need the low-down fundamentals
- The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity assessment standard from the Department of Defense (DoD) designed to further ensure that defense contractors at all levels are truly protecting sensitive defense information.
- When finalized, the requirements for CMMC will be added at 32 C.F.R. part 170
- The foundations: NIST SP 800-171 (Rev. 1/2/3)
  - Rev 1 – Previous
  - Rev 2 – Current
  - Rev 3 – Public comment period ended 26 January 2024
- Still relevant: DFARS 252.204-7012
  - Tell me why?

CMMC: 10 Things for the C-Suite

1. CMMC is a cybersecurity compliance regime that augments what is required by contractors and subcontractors doing business with the U.S. Department of Defense
2. CMMC will apply via phased roll-out to contracts and subcontracts that involve the processing, storing, or transmittal any information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government
3. CMMC ***does not*** apply to (1) contracts below the micro-purchase threshold (currently $10,000 in 2024) or (2) contracts exclusively for "commercially available off-the-shelf" (COTS) items, defined generally as any item of supply (including construction material) that is (a) a commercial item, (b) sold in substantial quantities in the commercial marketplace and (c) offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace
4. "Controlled Unclassified Information," or "CUI" includes a wide variety of information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using express safeguarding or dissemination controls
5. CMMC has three levels of requirements that DoD Program Managers will identify in solicitations based on the supplies and/or services being sought

CMMC: 10 Things for the C-Suite

6. CMMC Level 1 requirements are expected to apply to non-COTS DoD contracts over the micro-purchase threshold where the need to process, store, or transmit any CUI ***is not*** intended or expected
7. CMMC Level 2 requirements are expected to apply to non-COTS DoD contracts over the micro-purchase threshold where the need to process, store, or transmit any information that a law, regulation, or Government-wide policy requires or permits an agency to handle using express safeguarding or dissemination controls ***is*** intended or expected
8. CMMC Level 3 requirements are expected to apply to non-COTS DoD contracts over the micro-purchase threshold where the use of express safeguarding or dissemination controls ***are*** intended or expected to be used to process, store, or transmit any information that a law, regulation, or Government-wide policy requires or permits an agency to be protected by an adversary possessing sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (the "Advanced Persistent Threat")
9. Costly and lengthy self or third-party assessments, senior affirmations, and certifications given to the DoD will be required and DoD audits should be expected
10. CMMC requirements will need to be flown down to vendors and subcontractors at all tiers

CMMC: 10 Questions C-Suites Should Be Asking

1. Is our company a DoD contractor, subcontractor, or supplier?
2. Do we have a CUI Policy?
3. Are the clauses found at FAR 52.204-21, DFARS 252.204-7012, and/or DFARS 252.204-7021 resident in or referenced by any of our existing contracts, subcontracts, or supply/vendor agreements?
4. Does our System Security Plan reflect that our information system network is properly suited for segmentation in case we need to isolate DoD contract information?
5. How have we made any representations, via contract acceptance and invoicing, submissions pursuant to DFARS 252.204-7019 and -7020, Cyber Incident reporting pursuant to DFARS 252.204-7012, etc., to the DoD related to our cybersecurity?

CMMC: 10 Questions C-Suites Should Be Asking

6. What, if any, representations have we made to our stockholders/partners/subcontractors/prime contractors related to our cybersecurity?
7. Are we using or intending to use in performance of a DoD contract a Cloud Service Provider (CSP) to process, store, or transmit CUI or an External Service Provider (ESP) for the provision and management of comprehensive IT and/or cybersecurity services that will process, store, or transmit CUI or Security Protection Data on ESP assets?
8. How are we sure that our domestic and foreign supply chain is able to comport with the requirements resident in CMMC?
9. What changes are we prepared to make in our subcontractor responsibility and award assessments that comport with CMMC?
10. Are we using or intending to use in performance of a DoD contract or provide to the DoD Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment, Restricted Information Systems, or Test Equipment?

CMMC: 10 Questions w/no Present Answers

1. How much is all of this going to cost?
2. When will this be final and in my contract/subcontract?
3. How do I know for sure what CMMC Level will apply to me, my contract, or the products/services I supply?
4. When can I get formally certified by a third-party assessment organization?
5. Can I be assured that the Department of Defense will properly mark material they intend to be protected or define the required CMMC level for all tiers of subcontractors?

CMMC: 10 Questions w/no Present Answers

6. What is the impact should a prime contractor not properly or adequately identify the appropriate CMMC level in its subcontract?
7. What happens should a prime or subcontractor not be able to locate or identify a CMMC-compliant source?
8. How do I know if I'm being targeted by an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (an "Advanced Persistent Threat)?
9. What triggers, if any, can cause CMMC requirements to escalate/decrease among the three Levels over time?
10. Are there remedies available to challenge a negative CMMC Certification Assessment beyond the final decision of the Accreditation Body's final decision on elevated appeals?

Questions? We are here to help!

Alex Major
Partner
(202) 753-3440
amajor@mccarter.com

Franklin C. Turner
Partner
(202) 753-3432
fturner@mccarter.com

- Protests
- Claims
- REAs
- Teaming
- Joint Venture
- Anti-Collusion
- Cybersecurity/ CMMC
- CAS/Costs