Overview

For additional guidance, please refer to Steptoe’s COVID-19 Resource Center.

While attention is necessarily focused on the nation’s response to COVID-19, defense contractors should not put aside the need to prepare to meet DoD’s Cybersecurity Maturity Model Certification (CMMC) requirements. In fact, early this month the CMMC Accreditation Body announced on its website it had signed a Memorandum of Understanding (MOU) with DoD related to implementing CMMC, and is working to make more information about the agreement public. Even if DoD’s phased CMMC rollout is delayed, it is not likely to be materially changed. COVID-19 may provide immunity to those who go through it, and hopefully a vaccine for those who don’t, but these protections will not apply to cybersecurity threats to the defense industrial base. The rollout of these CMMC requirements is a matter of “when,” not “if.” Coupled with the structural change from self-certification to third-party audit, CMMC represents a sea change in the compliance requirements facing DoD contractors (and potentially those doing business with other government entities) that DoD contractors will be unable to implement overnight. DoD contractors – and their supply chains – should be proactive in responding to these requirements if they want to continue to do business with the Defense Department.

Background

In 2013, DoD issued a final rule mandating the inclusion of cybersecurity safeguarding and reporting requirements in all solicitations and contracts. In its current incarnation, DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting” (Dec 2019), the clause applies to “covered contractor information systems,” defined as “unclassified information systems” that “process, store, or transmit covered defense information.” Covered defense information, in turn, is defined as “unclassified controlled technical information or other information, as described in the Controlled Unclassified (CUI) Registry, that requires safeguarding or dissemination controls” and is either provided by or on behalf of DoD and identified in the contract or task order, or “collected, developed, received, transmitted, used, or stored” by the contractor in support of the contract. 7012(a).

The 7012 clause requires that all covered information systems must have “adequate security” – i.e., “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information” 7012(a). The baseline security requirements are those found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. The NIST standards set forth 14 families of security requirements, referred to as “domains.” Most requirements relate to policy and processes, and the secure configuration of IT, but several controls may require security-related software or hardware.

In addition, 7012(c) imposes rapid incident reporting requirements on contractors. Upon discovery of a cyber incident that affects a covered information system or covered defense information residing therein, or that affects the contractor’s ability to perform operationally critical support requirements of the contract, the contractor must conduct a review for evidence and analysis of the compromise of covered defense information, and rapidly report cyber incidents to DoD (within 72 hours of discovery).

Most significantly, the 7012 clause and NIST Standards rely on self-certification rather than third-party audits. Or, more precisely, they rely on self-noncertification – contractors (and subcontractors) must identify any variance from NIST SP 800-171 security requirements. 7012(b)(2)(ii)(B) and 7012(m)(2)(i).

CMMC
Cybersecurity threats aimed at the defense industrial base have grown, and DoD has concluded that contractor cyber defenses must be enhanced. Last year DoD began structuring the CMMC program, setting out five different levels of what it calls cybersecurity “maturity.” DoD is looking for “institutionalization,” which it describes as “the extent to which an activity is embedded or ingrained in the organization,” so that outcomes will be consistent, even at times of high stress. CMMC adds three “domains” not found in the NIST standards, and has a number of “practices” that are focused on situational awareness, cyber threat alerts, and cyber threat intelligence – which are not the focus of the NIST standards. Most significantly, the CMMC initiative moves away from contractor self-certification to a system where DoD will stand up a network of independent, approved CMMC third Party Assessment Organizations (C3PAO’s).[5]

On January 31, following several draft versions that received public comment, DoD released version 1.0 of the Cybersecurity Maturity Model Certification, including briefing slides, CMMC Version 1, and more than 300 pages of appendices (with detailed information and examples of processes and practices). It will be critical for DoD contractors and subcontractors to understand these requirements, and recognize how they differ from those contained in NIST 800-171, with which they may already be familiar.

Scale
First, consider the scale. DoD estimates that there are 300,000 DoD suppliers – contractors and subcontractors – who must receive CMMC certification in order to continue to do business with the department. While most will be subject only to the most basic “Level 1” CMMC requirements, the certification process alone will be an ambitious, bureaucratically burdensome undertaking, imposing potentially substantial new costs on defense suppliers. Because CMMC represents a sea change from DoD’s past practices in this space, defense contractors, and subcontractors should anticipate potential delays and disruptions, especially in the current environment. Before contractors can be certified, assessment organizations (C3PAO’s) must be created and trained. The CMMC Accreditation Body was established as a nonprofit organization in January 2020. Its goal is to train, test, and license[6] up to 10,000 CMMC assessors, supported by Carnegie Mellon University’s Software Engineering Institute (SEI) group. DoD has expressed its hope to have the first class of auditors trained by late April 2020.[7] It remains to be seen whether this timetable will be delayed by COVID-19, but DoD Chief Information Security Officer, Katie Arrington, has said[8] that “we are not slowing our roll at all.” Regardless of timing, these numbers bring to mind the labors of Hercules – and he didn’t have to wash his hands frequently or wear a mask.

Why is this Important to DoD Contractors?
The real teeth behind CMMC is DoD’s stated intention to require CMMC certification of all who want to contract with DoD. This process will be rolled out over several years. DoD has previously indicated it will include CMMC requirements in ten selected Requests for Information (starting in June 2020), which will evolve into formal Requests For Proposals (starting in September 2020). While this timetable may be delayed, the specified solicitations will require contractors to be CMMC-compliant by the time of contract award. The DFARS council is drafting a new solicitation provision to accompany this process.[9] CMMC requirements will not, however, be added to existing contracts.

And it doesn’t stop with contractors. Many procurements are likely to require contractors to “flow down” CMMC certification requirements to subcontractors. That means that prime contractors may have to encourage their teaming partners to become CMMC certified – and monitor their progress as they do so. That can raise challenging inter-company issues, since it is often the case that a teaming partner on one program is a competitor on other programs, generating a reluctance to share sensitive information (such as CMMC status).

But wait. There’s more. The latest DCMA Guidebook for Contractor Purchasing System Reviews has added standards for DCMA auditors to use to assess supply chain management complying with DFARS 252.204-7012. The new standards require contractors to demonstrate, among other things, how they determine that their subcontractors have information systems that can receive and protect Covered Defense Information, and how CDI is properly marked and securely transferred to subcontractors. In other words, if a defense contractor wants to maintain its Approved Purchasing System status (which can be critical to contracting success), it will have no choice but to engage in active management of subcontractor cybersecurity systems.

What are the Certification Levels?
CMMC uses a taxonomy that starts by sorting cybersecurity practices into different domains.[10] Within each domain are “capabilities,” which are further divided into “processes” and “practices” (which describe “activities”). Certification may be achieved at any of five different levels of increasing rigor. The requirements are cumulative – each level incorporates the requirements of lower levels.

Level 1 is termed “basic cybersecurity hygiene” – covering information provided by or generated for a government contract, and which is not intended to be made public. It is basically a restatement of the standards found in FAR 52.204-21. It is limited to 17 different practices, and is the baseline for any company doing business with DoD. The large majority of DoD contractors will be required to comply only with CMMC Level 1. This reflects DoD’s intention to strengthen the
cybersecurity maturity of smaller defense suppliers (while keeping them in the defense industrial base).

Level 2 represents an intermediate step, intended to protect Controlled Unclassified Information (CUI). It adds 55 controls or practices, including some but not all of the NIST 800-171 standards, plus seven other practices.

Level 3 represents “good cyber hygiene.” To achieve compliance with CMMC Level 3, suppliers basically need to comply with NIST 800-171 level of practices, plus 20 other practices. And keep in mind that Level 3 certification (unlike NIST 800-171 compliance) cannot be self-certified; the aspiring contractor must pass a third-party assessment confirming its cybersecurity maturity.

Levels 4 and 5, “advanced cyber hygiene,” are intended for contractors handling CUI associated with “critical programs and technologies,” and to address and reduce the risk from “Advanced Persistent Threats” – i.e., sophisticated adversaries. These levels include, respectively, 156 and 171 different controls or practices. Many of these practices go well beyond NIST 800-171. Some are based on NIST 800-171B (which is being renamed going forward to NIST 800-172), as well as other practices from the Center for Internet Security (CIS), CERT Resilience Management Model (CERT-RMM), and NIST Cybersecurity Framework (CSF).

An abridged version provided in CMMC 1.0 is:

**Level 1** – Select practices are documented where required [i.e., able to walk through small buildings via doors and hallways]

**Level 2** – Plus - each process is documented, and a policy exists for all activities [i.e., able to leap small buildings in several bounds]

**Level 3** – Plus - a plan exists and is maintained and resourced, that includes all activities [ i.e., able to leap small buildings in a single bound]

**Level 4** – Plus - activities are reviewed and measured for effectiveness. [i.e., able to leap medium-size buildings in two bounds]

**Level 5** – Plus – there is a standardized, documented approach across all applicable organizational units [i.e., able to leap tall buildings in a single bound]

**A Practical Example**

Let’s look at an example – the System and Information Integrity Domain. Per Appendix B of the CMMC 1.0, “System and Info Integrity activities insure that technology assets (e.g., desktops, software) that contain CUI are continuously monitored to detect violations of the authorized security state. Additionally, electronic mail (email), a common attack vector, is monitored and protected to detect malicious activity.”

The System and Information Integrity Domain requires four capabilities:

- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring
- Implement advanced email protections

CMMC 1.0 identifies the practices for each Level (with examples and references to applicable FAR, NIST, and other provisions) that are tied to these capabilities.

**Level 1** – Identify, report, and correct information system flaws in a timely manner; provide protection from malicious code and update that protection when new releases are available; perform scans of information system and files as they are downloaded. (Note – these are identical to the measures prescribed in FAR 52.204-21(b)(xii-xv)).

- Amplifying this list, the discussion of the first practice (identify, report, and correct flaws) identifies types of security-relevant updates and available external resources, including vendor updates and patch management. The example cites knowledge of the risks, enabling of all security updates, and purchasing maintenance packages for hardware and operating system.

**Level 2** adds – Monitor security alerts and take responsive action; monitor systems to detect attacks and potential attacks; identify unauthorized use. (These practices are found in NIST800-171)

**Level 3** adds – Employ spam protection, email forgery protections, utilize sandboxing. (These practices go beyond FAR and current NIST standards).

**Level 4** adds – Use threat indicator information and effective mitigations from external organizations to inform intrusion detection and threat hunting.

**Level 5** adds – Analyze system behavior to detect and mitigate execution of normal commands and scripts that indicate malicious actions; monitor individuals and components on an ongoing basis for anomalous or suspicious behavior.

**Training Guides**
Recognizing the complexity of the CMMC program, DoD is rolling it out in stages. DoD has planned a five-year phased rollout with increasing levels of complexity and certification, 15 practices are to be rolled out in 2020-21, then 75 in 2022, 250 in 2023, 479 in 2024, and another 479 in 2025. Training guides are intended to help companies understand what they have to do to meet certification requirements.

Takeaways

So what are the key takeaways from all this?

- Contractors and subcontractors should get ahead of the power curve. Be proactive in learning about CMMC requirements, and develop compliant policies and practices for the certification level you anticipate needing. This is a moving target, with much learning to come on the part of both DoD and industry. Don't wait for the audit to tell you what to do.

- Don't drag your feet. Don't run the risk of losing (or being disqualified from) a competitive procurement, or losing a contract award. Even worse, don't misstate your cybersecurity capability — it could lead to serious False Claims Act liability.

- CMMC can offer a competitive advantage as well. Early certification (as opposed to plans to get certified before the contract award date) can be a significant discriminator. Even if it is not listed as an evaluation factor in Part M of the RFP, reducing the uncertainty of future contractor certification can't help but make a Source Selection Official more comfortable.

- Finally, even if DoD is not a significant market for you, some civilian agencies (particularly Homeland Security), and even foreign governments, have been following the progress of the CMMC program and may decide to follow DoD's lead and adopt or adapt CMMC certification requirements as a model.

In conclusion, many questions remain to be answered over the next five years. How will C3PAO's measure compliance? How long will the process take? How will disputes or appeals be handled? Stay tuned!

[1] Three years later the FAR issued a rule, FAR 52.204-21, “Basic Safeguarding of Covered Contractor Information Systems” (JUN 2016), which specifies a minimum level of “basic safeguarding requirements and procedures to protect covered contractor information systems.”

[2] Cloud computing services are subject to a separate security clause. Additional requirements may be imposed in the contract itself, or if the contractor reasonably determines that additional security measures may be required to provide “adequate security” in a dynamic environment or to accommodate special circumstances.

[3] The NIST standards are themselves evolving.

[4] The requirements of the clause must be flowed down to subcontractors as applicable. 7012(m).

[5] Someone is a Star Wars fan. JEDI is already taken, but we are looking forward to Yearly Organization Data Security Audits (YODA’s). BABY YODA’s are probably not in the foreseeable future, however.


[10] CMMC adds three domains to the 14 found in NIST 800-171: for asset management, recovery, and situational awareness.


[12] For example, free briefings and webinars are offered by the CMMC Academy (https://www.celerium.com/cmmc-academy-for-defense-suppliers).

[13] For example, in the case of United States ex rel Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019), the court denied a motion to dismiss where the relator (whistleblower) alleged that the defendants failed to adequately address the vulnerability findings of an external information security assessment and falsely certified that it provided “adequate security” in connection with applicable cybersecurity requirements involving federal information in the contractor’s internal IT systems. The court found the allegations satisfied the “materiality” criterion of the False Claims Act. (The relator was the former head of cybersecurity for the defendant, and had been fired after refusing to sign documents that the company was in compliance with cybersecurity requirements, filing an internal report, and contacting the company’s ethics hotline.)