Pepper Hamilton LLP
Attorneys at Law

SERA-BRYNN
PCI QSA CYBER SECURITY SPECIALISTS

Government Contracts Cyber Café Series
Straight Talk on the DOD's Cybersecurity Maturity Model
June 9, 2020

SPEAKERS

- Hilary S. Cairnie, partner and chair, Government Contracts Practice Group, Pepper Hamilton LLP
- Heather Engel, principal and co-founder, Sera-Brynn

OVERVIEW OF WEBINAR

The Cybersecurity Maturity Model Certification (CMMC) Model and Appendices were released early this year, and this webinar covers all things CMMC. We will briefly cover the model, the term "FCI," and how to shift from DFARS 252.204-7012 to CMMC. Finally, we discuss how you can create useful documents that support the audit process, show cyber maturity, and provide legal top-cover instead of generating mountains of paperwork no one reads except at audit time.

We focus on the impact and application of CMMC to the Defense Industrial Base, although we also touch on preparing for an assessment.

Disclaimer: We do not address in these sessions the civilian agency counterpart regulations appearing at FAR Subpart 4.19.

Disclaimer: Our principal purpose in these sessions is to heighten your awareness of the many moving parts associated with DOD's regulatory framework for cyber compliance, but we are not providing legal or technical advice that is specific to your organization.

Reference Resources

- FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems
- DFARS 204-7300, DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 239.7600, DFARS 252.239-7010 – Cloud Computing

- DOD FAQs: https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf
- CMMC Model v1.02 and Appendices: https://www.acq.osd.mil/cmmc/draft.html
- DFARS 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting: https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

Overview

The CMMC is about **maturity**.

You must understand your business process to properly secure critical information. You cannot effectively prepare for the CMMC without a data management plan. And when preparing for an audit, keep in mind that you must have documented processes, and you must adhere to these processes.

CMMC: CURRENT STATUS

First, what is CMMC and what/where are related documents?

The Cybersecurity Maturity Model Certification will require a third-party inspection and certification of companies in the Defense Industrial Base (DIB). For the past several years, companies have self-attested under DFARS requirements. Successfully bidding on future contracts will require that a Certified Third-Party Assessment Organization, or C3PAO, validate that the CMMC capabilities and processes have been implemented and are functioning as intended.

Do not waste your time with an online search for CMMC — you will have to scroll through half a page of companies offering to help you get certified. Go right to the source: the Office of the Under Secretary of Defense for Acquisition & Sustainment, https://www.acq.osd.mil/cmmc.

As of the date of this webinar there are **no** CMMC Third-Party Assessment Organizations.

If you are interested in becoming an assessor or have questions about the assessment process, https://CMMCAB.org is the place to go.

Our recent discussion on the Commercial Off-the-Shelf (COTS) exception is worth a review as you prepare for CMMC because, as industry looks ahead to complying with CMMC, understanding your regulatory responsibilities (DFARS) is important to understanding your place in the supply chain, as well as the level of CMMC certification you may be required to obtain.

What Is in the CMMC Model?

The Model combines various standards and best practices to create maturity levels, ranging from Level 1 – Basic to Level 5 – Advanced.

Starting later in 2020 for selected contracts, defense contractors are required to undergo an audit that certifies they have met a minimum level of cybersecurity maturity. You will choose to certify at a level between 1 and 5. Most companies in the DIB will attempt Level 1; companies working with Controlled Unclassified Information (CUI) will need Level 3. Level 2 is transitioning and maturing processes. A company that will require Level 4 or 5 will typically be working on specific government technologies, and you are expected to have a substantial and proactive cybersecurity program (Level 4 definition) that addresses Advanced Persistent Threats (APTs). A company at Level 1 will have Federal Contract Information, or FCI.

FCI

If you have read through the CMMC, that may be the first time you have come across the term “FCI” or Federal Contract Information. If you have FCI, you must secure it to Level 1. Level 1 implements FAR 52.204-21. The DOD believes that most companies in the DIB will only require Level 1. FCI only requires minimum acceptable security requirements listed in the FAR clause and CMMC Level 1.

CUI

In March, the DOD released DODI 5200.48, Controlled Unclassified Information (CUI). This is the newest release on marking and handling CUI and incorporates new DOD marking guidance into research and plans. If your contracts include CUI, you will need to plan for certification at Level 3.

Pay attention to other designations in contracts — for example, statements in contracts that information must reside in a specific DISA SRG Level or additional requirements for Export Controlled Information.

CMMC Model Summary

CMMC has five maturity levels. Each level builds on the one before, so Level 3 includes all practices at Levels 1 and 2.

There are 17 domains. Each domain has capabilities and processes. Capabilities include practices. We will not cover in detail each of the domains — most of the domains map to NIST 800-171, and we have covered those extensively in this series.

However, there are three additional domains:

1. Asset Management
2. Recovery
3. Situational Awareness – supports risk-based decision-making and a common operational picture, staying up to date on emerging threats. An example of this would be the National Defense Information Sharing and Analysis Center.

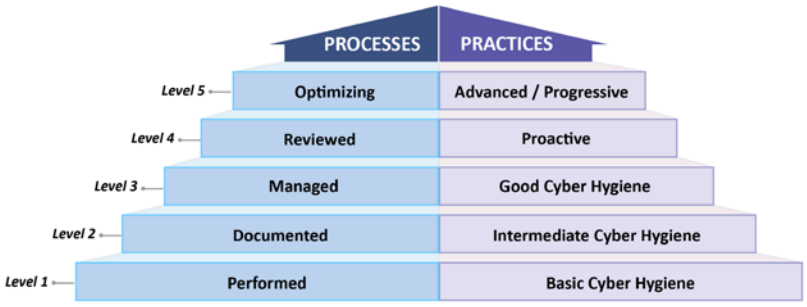

Figure 2. CMMC Levels and Descriptions

What Is the Purpose of CMMC?

CMMC is intended to add a verification component to DOD cybersecurity requirements. Under DFARS 252.204-7012, contractors self-attested that the acquisition clauses were met through acceptance of and continued work on the contract. Under CMMC, a third-party audit will be required.

How Does My Company Get Certified?

Wait until a process exists for certification. The CMMC Accreditation Board is up and running. The CMMC Accreditation Board will identify and certify auditors that will conduct CMMC audits. The accreditation body is a work in progress with several working groups. **There are no certified auditors at this time.**

Does CMMC Replace the FAR or DFARS Cyber Clauses?

DOD has proposed modifying 252.204-7012 or proposing a new regulation to address CMMC. As of May 2020, the proposed rule implementing the CMMC requirements is pending with the Office of Management and Budget's Office of Information and Regulatory Affairs. COVID-19 has created a challenge with holding public meetings, although the target date to issue a final rule by is October or November 2020.

Does CMMC Replace NIST Controls?

DFARS requires implementation of NIST 800-171 controls, and the NIST controls informed the Model versions, but CMMC Level 3 is not a one-for-one mapping to 800-171. There are additional controls and specific interpretations in CMMC Level 3. The DFARS cyber clause also includes specific procedures for incident reporting and use of cloud services, and CMMC includes additional practices in the IR domain.

When Should I Plan to Get Certified?

This year, the DOD projects 10 RFIs and 10 RFPs will require certification, for a total of approximately 1,500 companies under the Pathfinder program. Then, as contracts expire, expect new RFPs and awards to include it. Certification will be phased in over five years. Looking at the contracts you hold and when they expire will give you a sense of when you may need to be certified, as well as contracts you plan to pursue. So the short answer is: For some, it will be this year. For most it, will be 2021 — how early in 2021 depends on your business development strategy.

How Much Should We Budget for an Assessment?

This is unknown. It will depend on the level you plan to attempt and how prepared you are right now. Remember although the cost of security is

"allowable," that is not the same as "recoverable." We covered this in our September 2019 webinar, which you can listen to at https://www.pepperlaw.com/events/government-contracts-cyber-cafe-series-cybersecurity-costs-are-allowable-but-are-they-recoverable-2019-09-17/.

Beyond the cost of paying a third-party assessor, also consider the internal resources devoted to achieving and maintaining the level of maturity required. Many companies will require investments in technology. Something else to consider is whether your company will hold multiple certification levels for different business units or enclaves. An example would be a contract management system that might only hold FCI and a separate enclave specifically for processing CUI.

DOD stated back in April that for most companies it should cost $1,000 or less per year, however that assumes a Level 1 certification. And with a three-year accreditation cycle, it is unclear what other annual costs might be incurred.

Whom Should I Hire to Perform the Audit and Certify My Company?

The CMMC Accreditation Board is creating an audit standard and developing training for assessors. Once assessors are certified, there will be an authorized list to choose from. As of June 2020 — none of this exists, and any claims to be certified or able to certify you are false advertising. Stay away from those companies.

How Should I Prepare for an Audit?

The CMMC Accreditation Board is currently working on assessment standard documents that have been described as the "answers to the test," which will include how you apply the standard and the criteria for conformity. When these become available, that will provide the guidance to refining your documents and practices. That said, continuing to work on implementing NIST 800-171 plus reviewing and implementing the additional CMMC controls is a great way to mitigate risk and prepare for an audit, no matter what level your company plans to pursue.

Remember, CMMC is about **maturity**. Your practice must reflect the process as written. Auditors under most any framework are looking to see that you have documented processes and are following those processes (say what you do, do

what you say). Your SSP will remain an important and living document. CMMC also introduces different terms than we are used to with 800-171. Instead of controls and families, remember we now have **domains, capabilities, processes and practices** — your SSP will need revision to make sure the correct terms are used, and additional levels and domains added.

You cannot have open POAM items; however you will have a risk mitigation strategy (RM.3.146). A risk mitigation strategy acknowledges outstanding risk that your company wishes to address.

Your incident response plan must cover specific items in the IR domain. At Level 3, there are additional and more detailed items that previously required.

If I Am a DOD Contractor, Am I Included in DOD's DIB?

Yes, however as with DFARS, there is a COTS exception for companies selling **only** COTS products. (https://www.acq.osd.mil/cmmc/faq.html, question 19 and 20)

AUDIENCE QUESTIONS

Is this an enterprise-wide certification?

DOD acknowledged that it may be more realistic and efficient to assess CMMC maturity levels by segment or legal entity. This is good news for large companies with a mix of government and commercial revenue.

What about GCC High?

GCC High is not necessarily required to certify at Level 3. However, there may be situations where running your IT environment in GCC High is the most cost-effective and efficient solution — the answer depends. For example, if you use Microsoft 365 or Office 365 in the commercial space, there are a number of DFARS requirements that you will not be able to meet if you are protecting CUI. While we most often consider DFARS to be simultaneous with 800-171, there are additional requirements in the DFARS clause beyond 800-171, notably requirements around cyber incident reporting and cloud usage, as well as data center locations. GCC holds a FedRAMP Moderate designation; GCC High holds FedRAMP High. If you have ITAR or EAR data and your environment exists in the Microsoft cloud, Microsoft has stated that GCC does not meet the requirements for ITAR/EAR.

Would a "no CUI in the email" policy hold up, even though there is old CUI in the mailboxes?

In many instances, capabilities will be met with a policy. In this example, a policy stating that employees are not authorized to send or receive CUI is a good start, but, as an auditor evaluating maturity, I would then look for a few additional things. First, I would look for a verification mechanism — how will you know if an employee breaks the rule? Second, what is the response process for inadvertently receiving an email? And finally, old CUI data in mailboxes would need to be scrubbed. The presence of CUI in email when there is a policy stating no CUI in email is an indicator that the company is not following written processes.

Consultants and Auditors

DOD CISO stated earlier this spring that auditors will not be allowed to consult for companies they certify. There has also been discussion that auditors will not be able to sell products to companies they certify, *i.e.*, taking out the "easy button."

What steps can I take to prepare for CMMC?

We have two recommendations:

1. First, if you know security maturity could be better or you are working towards full DFARS compliance, keep going. Auditors are not only going to be looking at documented procedures but will be looking to see if your employees are following the procedures as written.
2. Second, run a tabletop exercise to see how CMMC might impact your supply chain. For example, if you build something for the government and you have a sole-source supplier, what is the impact on delivering that product if your sole-source supplier cannot or will not get certified? A supply chain working group that represents subcontracts, contracts, legal, internal program managers and others will not only help with CMMC but also with supply chain risk management.