Congress of the United States
U.S. House of Representatives
Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515–6315

MEMORANDUM

TO:	Members, Subcommittee on Oversight, Investigations and Regulations
FROM:	Dean Phillips, Chairman
DATE:	June 24, 2021
RE:	Subcommittee Hybrid Hearing: "CMMC Implementation: What It Means for Small Businesses."

The Committee on Small Business will meet for a hybrid hearing titled "CMMC Implementation: What It Means for Small Businesses." The hearing is scheduled to begin at **10:00 A.M. on Thursday, July 24, 2021, in person in 2360 Rayburn House Office Building and via the Zoom platform.**

The Cybersecurity Maturity Model Certification (CMMC) is a Department of Defense (DOD) initiative to increase cybersecurity preparedness across the defense industrial base. The hearing will provide Members the opportunity to learn more about this initiative, its implementation, and the compliance challenges it poses for small businesses.

Panel

- Mr. Jonathan T. Williams, Partner, PilieroMazza, Washington DC
- Mr. Scott Singer, President, CyberNINES, Madison, WI
- Ms. Tina Wilson, CEO, T47 International, Inc., Upper Marlboro, MD
- Mr. Michael Dunbar, President, Ryzhka International, Pompano Beach, FL

Background

Cyber-attacks are costly and threaten our national security. According to the Council of Economic Advisors, malicious cyber activity costed the U.S. economy between $57B and $109B in 2016.[1] In fact, cybercrime has grown exponentially, with reports estimating almost $1 trillion in global losses for cybercrime in 2020.[2] Just last April, the cyber-attack experienced by Colonial Pipeline Co., the largest fuel pipeline in the U.S., reminded us how cyberattacks can wreak havoc.[3]

[1] Off. of the Under Sec'y of Def. Acquisition and Sustainment, *"Cybersecurity Maturity Model Certification: Version 1.02"* (Mar. 18, 2020) https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf (herein CMMC V.1.02)
[2] Zhana Malekos Smith, et. al., McAfee, *"The Hidden Costs of Cybercrime"* (2020) https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[3] William Turton & Kartikay Mehrotra, Bloomberg, *"Hackers Breached Colonial Pipeline Using Compromised Password"* (Jun. 2021) https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Cybersecurity has become a key concern for the Department of Defense. Worried about the loss of sensitive defense information through cyber-attacks aimed at the over 300,000 companies that compose the Defense Industrial Base (DIB), the Department of Defense (DOD) created the Cybersecurity Maturity Model Certification.[4]

Overview of the Cybersecurity Maturity Model (CMMC)

CMMC is a framework that creates a "unifying standard for the implementation of cybersecurity across the Defense Industrial Base."[5] The main goal of the framework is to improve the protection of different types of unclassified information, such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).[6]

Once the initiative is fully implemented, it will be incorporated as a contractual requirement in almost all contracts with the DOD, with the exception of acquisitions exclusively for "commercial of the shelf " (COTS) items and acquisitions below the micro-purchase threshold ($10,000).[7] Thus, it will impact all those primes and subcontractors in the defense industrial base.

The CMMC framework consists of a tiered system and each level entails a series of processes and practices. The processes and practices in CMMC come from numerous cybersecurity standards and frameworks. [8]

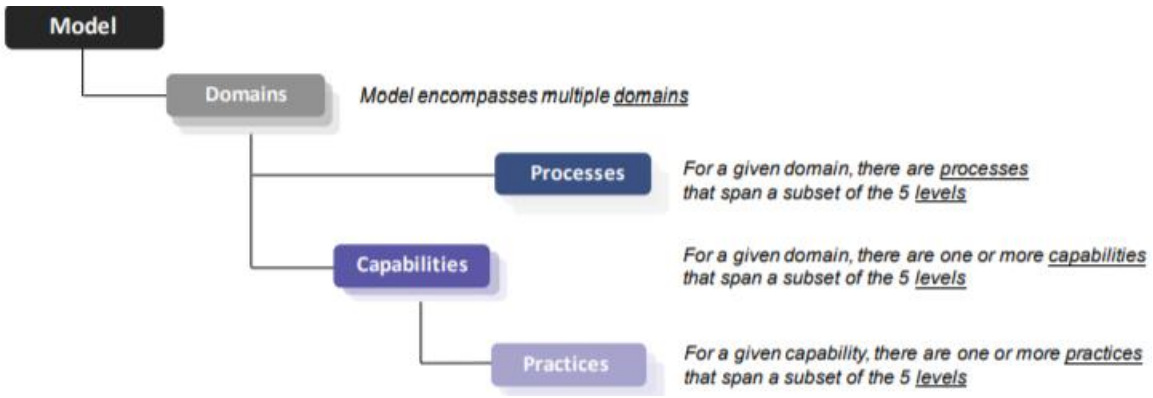
Currently, the Federal Government relies on contractual clauses to ensure contractor information systems that store FCI and CUI are adequately safeguarded. The first of these clauses is the Federal Acquisition Regulation (FAR) clause 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems" which protects FCI. The second one is the Defense Federal Acquisition Regulation (DFAR) clause 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting," which incorporates the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and seeks to protect CUI. The CMMC framework incorporates practices from these two clauses.[9] However, it changes the standard because contractors self-certify that they are in compliance with these contractual clauses, but under the CMMC framework they will need to obtain formal certification.[10]

How the CMMC Framework Works?

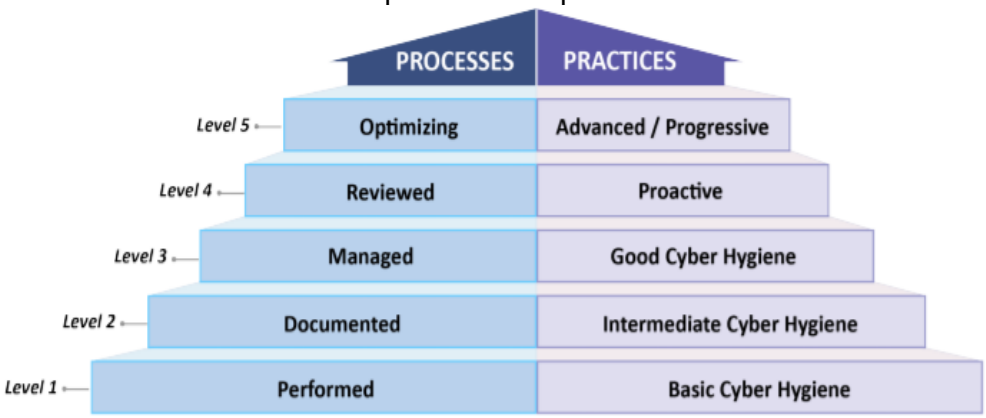
The CMMC framework has 5 levels and organizes interconnected requirements in two different ways. The first focuses on "domains" or categories of cybersecurity requirements. Each domain can be segregated into a series processes and practices that stretch across all 5 levels. Furthermore, "to provide additional structure," the framework organizes practices into different capabilities, within each domain.[11] The DOD diagram below provides a hierarchical organization of these concepts:

---

[4] CMMC V.1.02, *supra*, note 1
[5] *Id.*
[6] *Id.*
[7] Dep't of Def., *"Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019 -D041),"* 85 Fed. Reg. 61505-61522 (Sept. 29, 2020)
[8] CMMC V.1.02, *supra*, note 1
[9] *Id.*
[10] *Id.*
[11] *Id.*



To simplify matters, this memorandum concentrates on the first organizational arrangement, in which for each level, there is a series processes and practices. These practices range from level 1 "Basic Cyber Hygiene" to level 5 "Advanced". In parallel, the processes range from level 1 "Performed" and level 2 "Documented" all the way up to level 5 "Optimized". The DOD illustration below describes the practices and processes within each level:



To be certified at a certain level, a company must demonstrate both the implementation of practices (right side of the illustration) and the institutionalization of processes to ensure the implementation of such practices (left side).[12] Furthermore, the levels are cumulative. For example, in order for a company to obtain certification at a level 3, it also needs to demonstrate achievement of processes and practices at levels 1 and 2.[13]

The CMMC framework encompasses 17 domains, which translates into 171 practices in total.[14] As an example of how practices are mapped throughout the levels, let's take the first domain which is "Access Control". There are 26 practices associated to the "Access Control" domain- 4 at level 1, 10 for level 2, 8 for level 3 and so on.[15]

Out of the 171 practices, 110 come from the requirements specified in FAR clauses 52.204-21 and DFARS clause 252.204-7012.[16] In fact, level 1 is comparable to FAR clauses 52.204-21, including

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

all the requirements in that clause, plus two more practices. The same happens with Level 3. Based on its own practices and those in levels 1 and 2, Level 3 is comparable to the requirements in DFARS clause 252.204-7012, although it includes additional practices. [17]

Since the purpose of FAR clause 52.204-21 and DFARS clause 252.204-7012 is to protect FCI and CUI respectively, and those clauses are comparable to levels 1 and 3, it follows that CMMC level 1 aligns with the protection of FCI and Level 3 aligns with the protection of CUI.[18]

CMMC Certification Process

As mentioned, CMMC relies on third-party certification to assess the relative cybersecurity maturity of DIB companies. Thus, when the initiative is finally implemented and all contracts have requirements incorporating a specific CMMC level, only those contractors who have achieved the required CMMC level through the certification process will be eligible for award.[19] According to DOD plans, the intent is for the certification level to be stored in the Supplier Performance Risk System (SPRS) so that contracting officers can verify an offeror's certification level and currency prior to award.[20] CMMC certifications will be valid for 3 years.[21]

To receive the CMMC certification, all primes and subcontractors interested in doing business with DOD will need to be assessed by third party certifiers, commonly known as C3-PAOs.[22] C3-PAOs are trained and accredited by CMMC- Accreditation Body (AB), an independent and non-profit organization established to oversee the CMMC certification initiative.[23] There are multiple stages C3PAOs go through before getting the "accredited" status. To date, Redspin is the only company "authorized" to conduct CMMC assessments, which is one step prior to becoming fully accredited.[24]

Implementation Plans and Status

The DOD has long asserted that the CMMC initiative would be rolled out in a phased approach.[25] According to DOD plans, the initiative will be implemented on select contracts between FY2021-2025. During the first year, the initiative will be included in no more than 15 contracts, focusing on programs that require a level 3 assessment. In subsequent years, the initiative will be included increasingly in more contracts, with a few requiring levels 4 and 5. In specific, DOD anticipates including it in 75 for FY2022, 250 for FY2023, 325 for FY2024 and 475 for FY 2025. DOD expects to implement the program fully on FY2026.[26]

---

[17] *Id.*
[18] *Id.*
[19] Dep't of Def., *"Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019 -D041),"* 85 Fed. Reg. 61505-61522 (Sept. 29, 2020)
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] CMMC-AB, *"Frequently Asked Questions"* (Upd. May 2021) https://cmmcab.org/faq/
[24] CMMCAudit.org, *"C3PAO Authorization Levels Explained"* (June 2021), https://www.cmmcaudit.org/c3pao-authorization-levels-explained/
[25] *Supra*, note 19
[26] Off. of the Under Sec'y of Def. Acquisition and Sustainment, *"CMMC FAQs*" (Upd. Dec. 2020), https://www.acq.osd.mil/cmmc/faq.html

On September 29, 2020, the interim rule that allows DOD to include the CMMC in certain contracts became effective.[27] On March, under the direction of Deputy Secretary Hicks, DOD initiated an internal assessment of the CMMC initiative, which is guided by the following policy considerations: "Managing costs of cybersecurity for small businesses, clarifying cybersecurity regulatory policy and reenforcing trust and confidence in the CMMC assessment ecosystem."[28]

CMMC Challenges for Small Business

The CMMC poses multiple challenges for small businesses in different fronts. For example, many small businesses are concerned with the significant costs associated with the initiative, costs that will need to be incurred in preparation, during and post certification. These costs include hardware, software and associated labor; replacement of systems as they depreciate or become obsolete; labor costs in preparation for the assessment, to create protocols or to remain compliant; the costs of certifying and recertifying; and many more. The higher the CMMC level a small business wants or needs to achieve, the higher the costs. While DOD did provide an analysis of estimated costs relative to a small business implementing the different CMMC levels, those estimates have certainly been questioned for not including all associated costs and for being unrealistic.[29]

A challenge intimately related to costs is that many small businesses do not have the bandwidth to deal with the initiative. Many small businesses have very few employees wearing more than one hat. Thus, as a result, many small businesses will surely have to incur costs in specialists just to help them navigate the initiative. Furthermore, the probabilities of DOD compensating the costs associated with CMMC seem unlikely, particularly for subcontractors. According to DOD, the costs associated with implementing CMMC requirements, supporting the CMMC assessment and contracting with a C3PAO are allowable costs.[30] While it is not entirely clear how that would work, that seems intended for primes. When it comes to subcontractors, the one offering the lowest price is usually winner. Thus, if a subcontractor incurs more costs implementing CMMC than its competitors or if it seeks a higher CMMC level and its costs go up, it may not be selected.

There is also uncertainty as to CMMC as a flow-down clause. The Government will set the CMMC level required from primes. In turn, primes are supposed to flow down to subcontractors the appropriate CMMC requirement. The type of information the subcontractor will handle certainly serves as an objective factor to determine the CMMC level that should be flowed down because either the subcontractor handles CUI and needs levels 3, 4 or 5 or it does not and needs levels 1 or 2. However, within that, there is still discretion for primes to choose, leading to risk allocation issues and the fear that primes will ask the highest CMMC level they can from their subcontractors.

There are also concerns regarding the way companies will be prioritized to get the certification and whether there will be bottlenecks either in obtaining the certification or in accrediting C3PAOs as these challenges could represent an obstacle to firms getting certified and thereby being able to compete in DOD procurements.

---

[27] *Supra*, note 19

[28] Jesse Salazar (Deputy Assistant Secretary of Defense for Industrial Policy), "*Testimony on the Cybersecurity of the Defense Industrial Base before the Senate Committee on Armed Services, Subcommittee on Cyber"* (May 2021), https://www.armed-services.senate.gov/hearings/cybersecurity-of-the-defense-industrial-base

[29] See: Heidi Peters, Cong. Rsch. Serv., RL46643, "*Defense Acquisitions: DOD's Cybersecurity Maturity Model Certification Framework"* (Dec. 18, 2020).

[30] *Supra*, note 26.

Conclusion

The need for a more cyber-resilient DIB is unquestionable. However, equally important is to ensure that any initiative that intends to enhance the cybersecurity readiness of the DIB is not cost prohibitive or unduly burdensome, particularly for small businesses. Thus, the impacts of the CMMC initiative and any other comparable initiatives on the DIB should be closely examined. This hearing will serve to inform Members of the CMMC initiative and its effects on the DIB small business community.