Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base

Hala Strohmier
strohmierh@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Manoj Vanajakumari
vanajakumarim@uncw.edu

Ulku Clark
clarku@uncw.edu

Jeff Cummings
cummingsj@uncw.edu

Minoo Modaresnezhad
modaresm@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28412 USA

Abstract

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) published the Cybersecurity Maturity Model Certification (CMMC) framework in January 2020. The CMMC is a major federal effort intended to strengthen the ability of Defense Industrial Base (DIB) members to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). In this article, we briefly recount the history of unclassified information handling in the U.S. Federal Government that led to the current situation and explain why the CMMC was created, what it is, and what it entails. Through a series of interviews with a small sample of current large and small DIB members, we explore some of the perceptions, perceived challenges, and expected impacts of the CMMC on the DIB. We also consider the chances that the CMMC will accomplish its intended goals and describe a planned future larger study of the CMMC effort and its effects on the DIB.

Keywords: Cybersecurity Maturity Model Certification (CMMC)

1. INTRODUCTION

In February 2018, the Council of Economic Advisors (CEA, 2018) released a report that estimated the cost of malicious cyber activity to the U.S. economy in 2016 was between $57 and $109 billion. These costs stemmed largely from over 42,000 cybersecurity incidents that compromised the confidentiality, integrity, and/or availability (CIA) of information systems and

nearly 2,000 breaches resulting in confirmed unauthorized disclosure of data.

In addition to outright theft of intellectual property, there is concern, heightened since the 9/11 attacks, that the loss of many small pieces of seemingly insignificant information can aggregate to create a grave intelligence concern (Pozen, 2005). Referred to by some as the mosaic theory, this is where:

> Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts. (Pozen, 2005, p. 630)

Most of the data theft appears to be attributable not to a lack of effective security control guidance, but rather to poor cybersecurity habits and posture. Because of this, the Department of Defense (DoD) has embarked on an earnest effort to enhance the protection of sensitive data – especially among defense contractors. The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) worked with Johns Hopkins University Applied Physics Laboratory and Carnegie Mellon University Software Engineering Institute to create a new cybersecurity certification standard for DoD contractors. The goal of the new standard, named the Cybersecurity Maturity Model Certification (CMMC), is to provide cybersecurity guidance to the Defense Industrial Base (DIB) and hold them accountable for protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the supply chain.

Any vulnerabilities introduced to the supply chain ecosystem by the least cybersecurity-capable company weakens the cybersecurity posture of the entire supply chain since the chain is only as strong as the weakest link. Given the interdependencies between the systems of the customer (DoD), prime contractor, and sub-contractor(s), a breach of one can affect all. Use of a maturity model with built-in accountability is a way to reduce the inherent vulnerabilities stemming from the use of interdependent systems.

In this study, we investigate how ready the DIB is for the CMMC process by conducting a set of interviews with a group of small and large DoD contractors. We discuss the cybersecurity protocols and or standards currently in place in those companies, the current state of their cybersecurity posture, the CMMC level each company feels they need to achieve, concerns about achieving certification, and explore the differences reflected by the size of the company.

2. BACKGROUND

How to prudently handle non-classified information is something that the U.S. Government has wrestled with for quite some time. What follows is a brief history to set the stage and provide context from which the CMMC has emerged. President Carter's 1977 Presidential Directive to manage the security of unclassified telecommunications information transmitted among U.S. Government agencies and contractors, was arguably the first high-level U.S. policy dealing with unclassified information (Brzezinski, 1977). In 1984, this information was referred to as sensitive but unclassified (SBU) (National Security Decision Directive [NSDD], 1984) and later, was specifically defined as "information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests" (National Telecommunications and Information Systems Security Policy [NTISSP], 1986, p. 166). For the next 20+ years, the definition, handling, and sharing of SBU was problematic as was the proliferation of agency-specific labels for similar type information such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), etc.

Controlled Unclassified Information

In 2008, President G.W. Bush, in an effort to standardize government information handling practices and improve the sharing of information, issued a memorandum establishing a framework for managing CUI and coining the term CUI as

> the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as Sensitive But Unclassified (SBU) in the Information Sharing Environment (ISE), and establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI. (Bush, 2008)

Maintaining focus and momentum on this issue, President Obama issued a memorandum four months after inauguration that set up a task force

to review government procedures used to categorize and share SBU information as well as to consider measures for tracking government agencies' progress implementing the CUI framework (Obama, 2009). The task force report provided 40 recommendations, key elements of which were included 15 months later in Executive Order 13556 which also broadened the scope of CUI to include all SBU information within the Executive Branch (Holder & Napolitano, 2009; Exec. Order No. 13556, 2010).

After nearly four years of work to codify the CUI program, the Information Security Oversight Office, an organizational component of the National Archives Record Administration (NARA) which is the Federal Government's Executive Agent (EA) for CUI, issued a rule to establish policy for executive branch agencies on "designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI" as well as other aspects of the CUI program (Federal Register, 2016b). The guidance entered the Code of Federal Regulations) creating the CUI registry, which currently has 125 categories of CUI, and formally establishing the definition of CUI (Electronic Code of Federal Regulations [e-CFR], 2021; National Archives, 2020). Controlled Unclassified Information (CUI) is defined as:

> 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 safeguarding or dissemination controls. (e-CFR, Title 32, Vol. 6, Part 2002.4(h), 2021)

Contractor Protection of CUI

Around the same time, the DoD published a final rule on the DFARS clause requiring that contractors implement the security requirements in NIST SP 800-171 no later than December 31, 2017 (Federal Register, 2016a). Two key problems with this guidance were that (1) DoD had no process for certifying compliance (contractors could simply self-attest to their compliance) and (2) contractors were allowed to continue providing goods and services even if they were not fully compliant with 800-171 so long as any gaps were documented in a Plan of Action and Milestones (POAM) (National Institute of Standards and Technology [NIST], 2018).

Because of problems with implementation of Defense Federal Acquisition Regulation Supplement 252.204-7012 (DFAR, 2019), the Under Secretary of Defense for Acquisition and Sustainment issued a memorandum in January 2019 that directed the Defense Contract Management Agency (DCMA) to "validate compliance with the requirements of DFARS clause 252.204-7012" for certain contractors (Lord, 2019). As a direct result, DCMA stood up the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) in June 2019 to begin conducting assessments of some of the DoD's largest contractors (Tremblay, 2019).

Birth of the CMMC

The OUSD(A&S) announced in May 2019 the initiative to create the CMMC framework (Doubleday, 2019). Figure 1 depicts the key events in the CMMC development and implementation timeline.

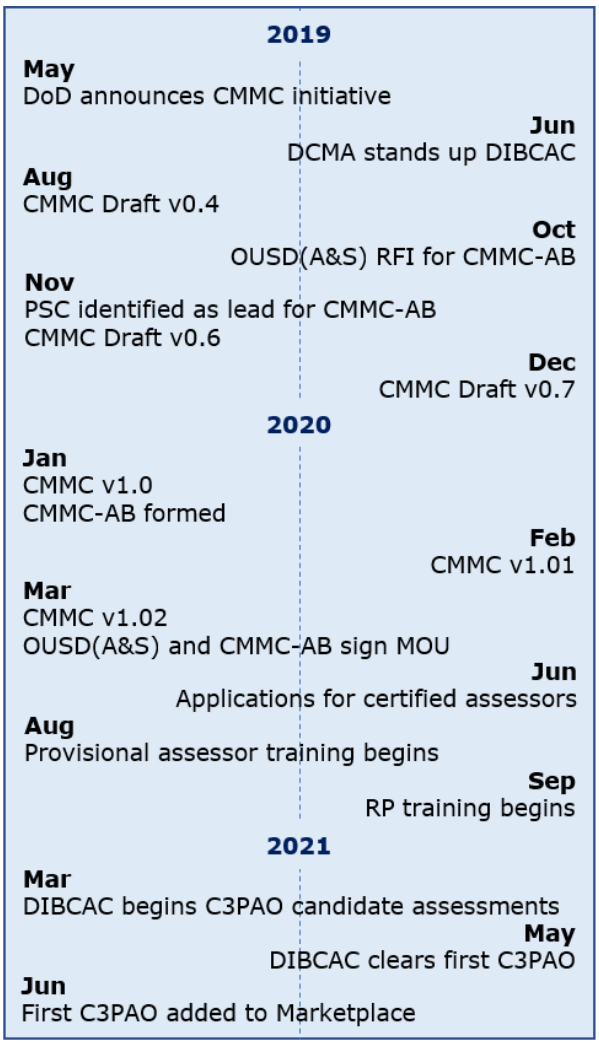

Figure 1 – CMMC development key event timeline

As some in the DoD iterated through draft versions of the CMMC, others worked to create

the organizational structure required to implement it. In early October 2019, the OUSD(A&S) published a request for information (RFI) on "how to define the long-term implementation, functioning, sustainment, and growth of the CMMC Accreditation Body (RFI HQ0034SS10032019, 2019). In November 2019, an Accreditation Body kickoff meeting was held out of which the Professional Services Council (PSC, 2021) emerged as the lead to create a volunteer board to establish a nonprofit to act as the accreditation body for the CMMC process (Barnett, 2020). The PSC, founded in 1972, is the 400+ member-company national trade association of the government technology and professional services industry providing federal agencies with services.

The CMMC Accreditation Body (CMMC-AB) formed as a non-profit organization in January 2020 with a 15-person volunteer board and signed a formal Memorandum of Understanding (MOU) with the OUSD(A&S) in March 2020 (Lord & Schieber 2020). The CMMC-AB manages and oversees all certification, training, and accreditation aspects of the CMMC including training of Registered Practitioners (RPs); marketplace listing of Registered Provider Organizations (RPOs); accreditation of CMMC Third Party Assessment Organizations (C3PAOs); and, most importantly, contractor CMMC certification.

Key to getting 300,000 defense contracting companies through the certification process over the next several years are the C3PAOs. Each C3PAO must be Level 3 certified (CMMC Accreditation Body [CMMC-AB], 2021) by DIBCAC and meet various administrative and personnel requirements from the CMMC-AB before they can begin conducting contractor assessments. DIBCAC assessments of C3PAOs, which began in March 2021 (Goepel, 2021), take approximately 6 weeks, including scheduling and pre-assessment reviews, virtual and on-site assessments, and post-assessment analysis. The CMMC-AB Marketplace reflected in early June 2021 that there were 156 C3PAO candidates pending Level 3 assessment and a single company, Redspin, officially designated as a certified assessment organization.

3. CMMC Details

The CMMC is a framework designed to provide the DoD with verification that DIB members can adequately protect FCI and CUI flowing through the supply chain from customer to prime contractors to sub-contractors. It builds upon existing regulations, other models' best practices, and combines multiple existing cybersecurity standards both from within the U.S. government and internationally (DoD, 2019).

CMMC Components

Based on early work conducted by the Software Engineering Institute to improve software processes (Paulk, et. al, 1993), the framework uses five levels to designate an organization's cybersecurity maturity. Each of these levels is defined by the *processes* an organization has established and is following, as well as the *practices* that are implemented. This relationship between processes and practices across the five maturity levels of the CMMC is reflected in figure 2. Processes range from Performed, at level 1, to Optimizing, at level 5. With CMMC required practices in place, level 1 is considered Basic Cyber Hygiene, while level 5 is Advanced/Progressive. An organization certified at any level of the CMMC is meeting the processes/practices of that level as well as those below it.

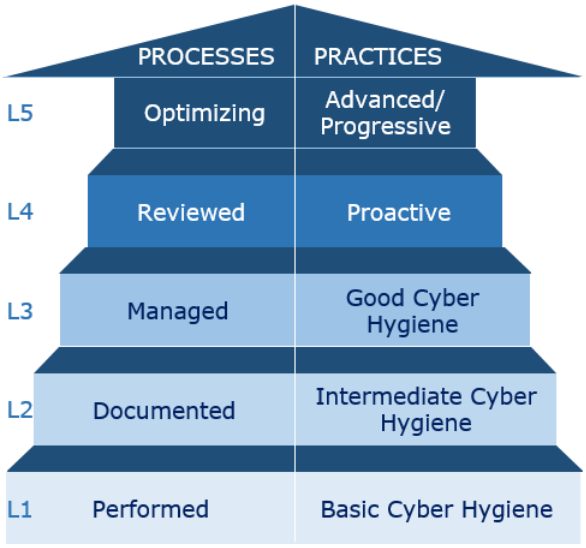

Figure 2 – CMMC processes and practices at each maturity level

General meanings/descriptions of the five levels are as follows:

- Level 1: Protecting FCI is the focus and is achieved by meeting the basic requirements of 48 CFR 52.204-21.
- Level 2: This level represents a transitional stage for organizations working towards Level 3. The focus is on replacing ad-hoc processes/practices with well-documented processes and corresponding regular practices.

- Level 3: Protecting CUI is the focus and is achieved with well-established processes accompanied by implementation of all regular practices outlined in NIST SP 800-171, plus 20 additional practices.
- Level 4: This level could be viewed as a transitional stage for organizations working towards Level 5. Reviewing and measuring existing practices to gauge effectiveness and enhancing security to protect CUI from Advanced Persistent Threats (APTs) is the focus.
- Level 5: At this highest level, organizations would be continually optimizing existing processes and practices. Being capable of defending CUI from APTs would include, among other things, such practices as noticing missing logs, verifying the integrity of security critical software, responding in real-time to anomalous network activities, and recording network traffic crossing organizational boundaries.

The number of practices that must be met and verified at each level are depicted in figure 3. Note that each level requires all practices from previous levels. For example, Level 1, Basic Cyber Hygiene, requires 17 practices be met, while Level 2, Intermediate Cyber Hygiene, requires 72 practices be met, 17 from Level 1 plus 55 from Level 2 (17 + 55 = 72).

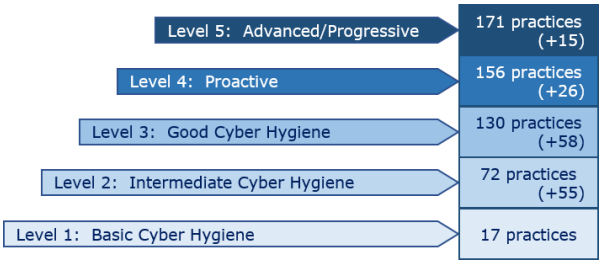

Figure 3 – number of practices required at each CMMC maturity level

As the goal of CMMC is to change the supply chain culture, every DIB member will need to be at least Level 1 certified. As emphasized by the OUSD(A&S) CISO:

> Level 1 reflects the basic cyber hygiene skills that we should be using every day, regardless. I've been asked, "Ma'am, I do landscaping for the government. Should I have CMMC certification?" And my answer has actually been, "Yes, I want you to at least get to Level 1". (Anderson, 2020).

The CMMC framework organizes practices within 17 domains, which includes the 14 domains enumerated in NIST 800-171 as well as 3 additional domains: Asset management (AM), Recovery (RE), and Security Assessment (CA). These domains are listed in table 1 where we present a crosswalk of the number of required practices across domains and levels. A crosswalk is a way of comparing or contrasting data.

The 17 practices (see Appendix B) required for Level 1 certification come from just 6 of the 17 domains while at Level 3, organizations must meet practice requirements across all 17 domains. The 17 domains are: Access Control (AC), Asset Management (AM), Audit and Accountability (AU), Awareness and Training (AT), Configuration Management (CM), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Personnel Security (PS), Physical Protection (PE), Recovery (RE), Risk Management (RM), Security Assessment (CA), Situational Awareness (SA), System and Communications Protection (SC), System and Information Integrity (SI).

Cybersecurity Practice Crosswalk by Domain and Level						
DOMAIN	L1	L2	L3	L4	L5	Domain Totals
AC	4	10	8	3	1	**26**
AM			1	1		**2**
AU		4	7	2	1	**14**
AT		2	1	2		**5**
CM		6	3	1	1	**11**
IA	2	5	4			**11**
IR		5	2	2	4	**13**
MA		4	2			**6**
MP	1	3	4			**8**
PS		2				**2**
PE	4	1	1			**6**
RE		2	1		1	**4**
RM		3	3	4	2	**12**
CA		3	2	3		**8**
SA			1	2		**3**
SC	2	2	15	5	3	**27**
SI	4	3	3	1	2	**13**
Totals	17	55	58	26	15	**171**

Table 1 – domain crosswalk for the number of required practices at each level.

CMMC Phased Implementation

The DFARS Clause 252.204-7021 states that OUSD(A&S) must approve the use of the clause for new acquisition until October 2025 after which

CMMC is expected to be fully implemented and required of all new contracts. Table 2 illustrates the roll-out plan over the next five fiscal years for the number of contracts that will contain a CMMC requirement. Table 3 shows the initial CMMC roll-out numbers of prime contractors and sub-contractors across that same time horizon.

Number of Contracts with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

Table 2 – CMMC roll-out by # of contracts

Costs associated with acquiring and maintaining certification will vary by the level of the certification and the size of the organization. The availability of resources among DIB is a concern that we noted during our interviews with the pilot group of small and large DoD contractors. We also noted that there was a consensus among most of the pilot study group regarding the importance of CMMC and the security it will add to the CUI and FCI data.

	Number of Prime/Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
L1	895	4,490	14,981	28,714	28,709
L2	149	748	2,497	4,786	4,785
L3	448	2,245	7,490	14,357	14,355
L4	4	8	16	24	28
L5	4	6	16	24	28
Tot	1,500	7,500	25,000	47,905	47,905

Table 3 – CMMC roll-out by # of contractors

4. METHODOLOGY

To investigate DIB understanding of, readiness for, and opinion of the CMMC process, we conducted interviews with 10 defense contractors: six small and four large businesses. Company size was established using Small Business Administration (SBA) standards related to number of employees and/or average annual receipts according to their North American Industry Classification System (NAICS) code (NAICS Association, 2019). It should be noted that there is no medium-size category in SBA classification of companies. All interviews were transcribed in their entirety and kept anonymous.

The 10 companies we interviewed were a convenience or opportunity sample. While the sample is nonrandom, we tried to include a mix of industries and blend of large and small companies to provide a reasonable approximation of the larger contractor population. The interviewees were mid-level managers of information technology departments or decision makers of small companies that outsource information technology needs. The open-ended survey questions were designed to collect information on the nature of the firms, their readiness for CMMC assessment, and their concerns. Appendix A lists the survey questions used in the interviews.

5. SURVEY RESULTS AND DISCUSSION

From the interview results, we note generally that all four large businesses in our pilot study have conducted several discussions regarding CMMC and have formed teams that include information security specialists assigned specifically for the CMMC adoption. Small businesses, on the other hand, had widely ranging responses from "we are starting to analyze the current state" to "almost compliant with our desired CMMC level." It was apparent from the responses that the small businesses that do not primarily provide information technology consulting services were struggling the most with CMMC.

In the following subsections, we discuss the responses to key questions (3, 4, 5, 6, 7, 9, & 10) from among the 10 asked.

Other Cybersecurity Framework Adoption

Responses to question 3, *Has your company adopted a cybersecurity framework or standard, if so, which one?*, indicate familiarity with cyber-related standards generally and some existing standards specifically. Given the DFARS clause deadline of December 31, 2017 that currently applies to all DoD contractors, this is not surprising and probably should have been a reason for greater awareness. Frameworks mentioned include (in no particular order): NIST Risk Management Framework (RMF), ISO 27001, NIST 800-171, Capability Maturity Model Integration (CMMI) Level 2, Payment Card Industry Data Security Standard (PCI DSS), Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act (HIPAA) provisions, Health

Information Technology for Economic and Clinical Health (HITECH) requirements, and CMMC.

Providing these standards in response to a question about "cybersecurity frameworks" may cause some concern/questions by readers, but it was insightful for researchers both to see familiarity with implementing governance requirements and for how some companies seemingly lumped many requirements into a single, large mental bin. Three (3) companies have not formally adopted any cybersecurity framework, though they are aware of the importance of cybersecurity practices generally and are loosely following them in an ad-hoc manner. These findings would seem to validate concerns of compliance with self-attestation.

CMMC Level Targeted

Question 4 asked companies: *Which CMMC Level (1-5) does your organization need per current/anticipated DoD contracts? What CMMC Level is your Prime requiring [if applicable] of your company?* Three of the four large companies indicated that they believe they currently meet level 3 certification requirements, while one was unsure of their status and likely does not yet meet level 1.

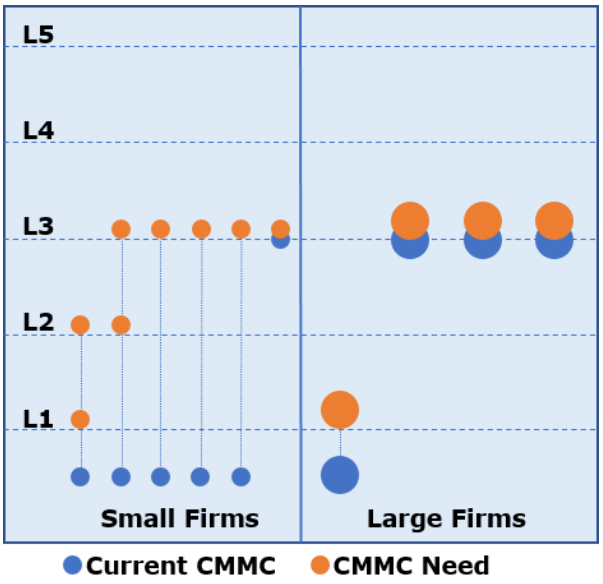

Figure 4 – pilot study group of 10 companies self-attested current CMMC level and future required level

One small firm indicated they were already meeting level 3 requirements, while none of the others professed to be currently meeting any level. All small companies seemed to understand the importance of achieving CMMC and were considering how to get to the level they felt they needed. Figure 4 shows the current CMMC readiness level attested by the pilot study group as well as the future desired/anticipated level.

Note the clear differences in the current readiness posture between small and large businesses. It seems readily apparent that small businesses will struggle more with the new CMMC mandate, specifically the ones performing in industries outside the cyber domain, while most large businesses appear positioned to rapidly meet the new requirements.

When asked about plans to continue to level-up on CMMC, two of the large firms stated they will likely push to levels 4 and 5 even if not required by contract. Two of the small firms expressed a view toward taking the CMMC levels in steps – get certified at level 1, then work on level 2, etc.

Short-term CMMC Achievement

In response to question 5, *what CMMC Level can your organization achieve in the short term (within 12-18 months)?*, all of the large contractors and cyber-focused small contractors interviewed had a good understanding of the requirements, budgeted CMMC readiness and certification costs, and had a plan to achieve the required certification level within the next 12-18 months. It was common among the small non-cyber companies that they had a more loosely sketched plan to get their systems ready. This could be linked to the lack of understanding by the leadership in those businesses of the cyber systems used in their companies and what it takes to meet the required CMMC levels. All companies interviewed understood the need to achieve CMMC in order to continue doing business with DoD.

Cost Concerns

Question 6 got into the question of CMMC cost: *Has your organization budgeted for CMMC costs? If yes, approximately how much, if no, why not? Please, choose a range: $0-$25k, $26k-$50k, $51k-$75k, $76k and above.* All companies had concerns regarding the CMMC costs. Note that the NAICS code provides a lower bound on the number of employees required to be classified as a large organization. Thus, the number of employees in a large firm can vary significantly. In other words, two large firms having employee numbers differing by tenfold would not be surprising. For that reason, it is hard to enumerate the anticipated cost per employee with the sample size. Without exception, all companies, large and small, were concerned about the resources and the cost of this new mandate. They were concerned not only about

the initial cost to bring their processes and practices up to certification standards, but also the ongoing cost of maintaining the certifications. The CMMC financial outlay suggested by the large businesses varied from $600K to $3M for the initial certification, while the small businesses' estimates ranged from $1K to $50K. While most companies expressed their willingness to do whatever it takes to keep working with DoD, they also expressed that the cost of tools/licenses that provide functions to maintain the certification would be an internal challenge as it will exceed what they normally spend for cybersecurity.

Little Concern about Inability to Adapt

For question 7, *is your organization concerned that it will not be able to adapt to CMMC required changes? What are your concerns (e.g., leveling up, losing contract)?*, the overriding theme of the response was that companies expressed willingness to do whatever it takes to keep working with DoD. An interesting concern voiced by some of the larger companies was the possibility of being held responsible for getting/keeping sub-contractors certified. In previous work by some of the authors (Vanajakumari, Mittal, Stoker, Clark, & Miller, 2021), this idea was proposed and, according to some of the interviewees' comments, it may be gaining traction among some in the DoD. The concern is understandable, especially if a small company is awarded as the prime contractor and a large company is a sub. However, generally, we continue to believe that in the highly interconnected cyber environment of today, the lead contractor (typically the more powerful member) must take special initiative and leadership to ensure the highest level of cybersecurity attainment.

Will CMMC Help?

Question 9 asked, *do you think CMMC will help your organization, or the supply chain of which you are a part, mitigate cybersecurity risks?* While all the companies in the pilot-group expressed a degree of cybersecurity concern and agreed that there is a need to secure supply chain data, three were not sure about CMMC helping. The responses from the three that had low enthusiasm for CMMC ranged from probably not to possibly. The lack of excitement among this subset mostly stemmed from confidence in their own current cybersecurity posture, which caused them to see CMMC as yet another top-down driven requirement that had little value to add. 80% of the companies interviewed believed that CMMC would certainly help in ensuring accountability when it comes to supply chain cybersecurity.

Final Interviewees' Thoughts

Outside the context of the 10 questions, the interviewed DIB members generally agreed that the third-party assessment will help with keeping businesses honest and thus complying with the cybersecurity requirements at the certified level. However, there were doubts expressed regarding the extent to which complying with CMMC practices would actually help avoid and/or contain cybersecurity events. Some of the concern stems from the fact that CMMC compliance is only checked once every three years and thus the reliability of compliance in between certification periods might be questionable.

6. CONCLUSIONS AND FUTURE WORK

To investigate the CMMC readiness of DoD contractors and sub-contractors, we conducted a pilot survey of 10 large and small government contractors. Our findings show that all DIB members are aware of the compliance requirements; however, their state of readiness and understanding of the certification requirements vary markedly depending on their size and the nature of their business. In light of some items revealed by our pilot study, like the respondents' concerns with contractors maintaining a proper cybersecurity posture during the three years between required certifications, we plan to conduct a follow-on CMMC study. That investigation will include more companies and delves more deeply into some of the questions raised from this pilot study regarding the differences in preparedness between small and large contractors.

On May 12, 2021, Presidential Executive Order 14028 was signed outlining the desired path to improve the nation's cybersecurity posture and protect federal government networks (Exec. Order No. 14028, 2021). Recent high-profile attacks (SolarWinds, Microsoft Exchange, the Colonial Pipeline, and JBS) reveal how vulnerable federal and private sectors are to cyberattacks from other nations and cyber criminals. Executive Order 14028 specifically requires implementation of some items, such as multi-factor authentication (MFA), that are currently part of CMMC Level 3, as a base requirement. This seems to signal that there might soon be some modifications to the list of CMMC controls at each level and that the CMMC framework might soon become more generally applied to other parts of the federal government.

There is also an increasing number of ransomware attacks cutting across all sectors. On June 3, 2021, White House released a memo

asking business leaders to step up their cybersecurity measures. Even though currently CMMC compliance is a requirement for DIB members only, in the light of recent events it is expected to become a standard for all U.S. businesses. Many attacks can be prevented by companies adopting CMMC Level 1 (basic cyber hygiene). Our findings provide insights to companies on the challenges associated with improving their cybersecurity stance.

Limitations of the Study

As mentioned previously, the intent of this study was to serve as a pilot to inform future studies on CMMC. However, this may be considered a limitation of the current results due to the size of the study (i.e., 10 companies). Additionally, based on feedback, some questions may need to be modified in future studies to elicit clearer responses. For example, questions surrounding budgeting for CMCC costs were asked without placing time constraints (e.g., have you budgeted for CMMC adoption in the next 12 to 18 months). These limitations will be addressed in future studies.

7. REFERENCES

Anderson, M. (2020, October 6). SME. *Your Best Cyber Defense Isn't a '60's Super Spy. It's You*. https://www.sme.org/technologies/articles/2020/october/your-best-cyber-defense-isnt-a-60s-super-spy.-its-you/

Barnett, J. (2020, June 23). FedScoop. The DOD wants better cybersecurity for its contractors. The first steps haven't been easy. https://www.fedscoop.com/cmmc-dod-cyber security-requirments-contractors-timeline/

Brzezinski, Z. (1977, November 16). Presidential Directive/NSC-24. Telecommunications Protection Policy. https://fas.org/irp/offdocs/pd/pd24.pdf

Bush, G. W. (2008, May 7). Memorandum for the Heads of Executive Departments and Agencies. *Designation and Sharing of Controlled Unclassified Information (CUI)*. https://fas.org/sgp/bush/cui.html

Council of Economic Advisers. (2018, February). *The Cost of Malicious Cyber Activity to the U.S. Economy*. https://www.hsdl.org/?abstract&did=808776

CMMC Accreditation Body. (2021, June). Cybersecurity Maturity Model Certification. https://cmmcab.org/

Defense Federal Acquisition Regulation. (2019). *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Supplement 252.204-712). https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

Department of Defense. (2019, November 7). Cybersecurity Maturity Model Certification (CMMC) Draft V0.6. https://www.acq.osd.mil/cmmc/docs/CMMC-V0.6b-20191107.pdf

Doubleday, J. (2019, June 3). *Defense Dept. to require new cybersecurity certification from contractors*. Inside Cybersecurity. https://www.the-center.org/getattachment/Our-Services/Cybersecurity-Services/Cybersecurity/Defense-Dept-to-require-new-cybersecurity-certification-from-contractor-2.pdf.aspx?lang=en-US

Electronic Code of Federal Regulations. (2021, May 27). *Controlled Unclassified Information* (Title 32, Vol. 6, Part 2002.4(h)). https://www.ecfr.gov/cgi-bin/text-idx?SID=54ce48937eb0b451c823363c49411eb2&mc=true&node=pt32.6.2002&rgn=div5#se32.6.2002_14

Exec. Order No. 13556, 3 C.F.R. 267 (2010). https://www.govinfo.gov/content/pkg/CFR-2011-title3-vol1/pdf/CFR-2011-title3-vol1-eo13556.pdf

Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021). https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Federal Register, 81 FRM 72986. (2016a, October 21). *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*. https://www.govinfo.gov/content/pkg/FR-2016-10-21/pdf/2016-25315.pdf

Federal Register, 81 FR 63323. (2016b, November 16). *Controlled Unclassified Information*. https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

Goepel, J. (2021, April 28). *DIBCAC Releases C3PAO CMMC Maturity Level 3 Lessons Learned*. CMMC Information Institute. https://cmmcinfo.org/2021/04/28/dibcac-releases-c3pao-cmmc-maturity-level-3-lessons-learned/

Holder, E. & Napolitano, J. (2009, August 25). Report and Recommendations of the

Presidential Task Force on Controlled Unclassified Information. https://www.archives.gov/files/cui/documents/2009-presidential-task-force-report-and-recommendations.pdf

Lord, E. (2019, January 21). Under Secretary of Defense for Acquisition and Sustainment Memorandum. *Addressing Oversight as Part of a Contractor's Purchasing System Review*. https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf

Lord, E. & Schieber, T. A. (2020, March). Memorandum of Understanding (MOU) between the Department of Defense, Office of the Undersecretary for Acquisition and Sustainment (OUSD(A&S)) and Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB). https://assets.documentcloud.org/documents/6935675/CMO001673-20-CMMC-AB-MOU-Fully-Executed-20200323.pdf

National Archives. (2020, April 13). *CUI Categories*. https://www.archives.gov/cui/registry/category-list

National Institute of Standards and Technology. (2018, December). *Risk Management Framework for Information Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Security Decision Directive Number 145 (1984, September 17). *National Policy on Telecommunications and Automated Information Systems Security*. https://fas.org/irp/offdocs/nsdd145.htm

National Telecommunications and Information Systems Security Policy. (1986, October 29). *National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems* (No. 2). https://www.princeton.edu/~ota/disk2/1987/8706/870611.PDF

North American Industry Classification System Association. (2019, August 19). SBA Table of Small Business Size Standards. https://www.naics.com/sba-size-standards/

Obama, B.H. (2009, May 27). Presidential Memorandum. *Classified Information and Controlled Unclassified Information*. https://obamawhitehouse.archives.gov/the-press-office/presidential-memorandum-classified-information-and-controlled-unclassified-informat

Paulk, Mark., Curtis, William., Chrissis, Mary Beth., & Weber, Charles. (1993). *Capability Maturity Model for Software (Version 1.1)* (CMU/SEI-93-TR-024).

Pozen, D. E. (2005). The Mosaic Theory, National Security, and the Freedom of Information Act. Yale LJ, 115, 628. https://www.yalelawjournal.org/pdf/358_fto38tb4.pdf

Professional Services Council. (2021). https://www.pscouncil.org/

Request for Information (RFI) HQ0034SS10032019. (2019, October 3). RFI Cybersecurity Maturity Model Certification Accreditation Body. https://sam.gov/opp/4a4b539a0e347e540b30b3121916031c/view

Tremblay, P. (2019, June 24). Defense Contract Management Agency (DCMA) website article. *Building a cybersecurity assessment capability*. https://www.dcma.mil/News/Article-View/Article/1885182/building-a-cybersecurity-assessment-capability/

Vanajakumari, M., Mittal, S., Stoker, G., Clark, U., & Miller, K. (2021). Towards a Leader-Driven Supply Chain Cybersecurity Framework. JISAR, 14(2), 42. http://jisar.org/2021-14/n2/JISARv14n2p42.pdf

Appendix A – Survey Questions

(*Alt + Left arrow to return to hyperlink location*)

1. Which industry does your organization primarily support?
2. What is the size of your organization (small/large)? What is your main NAICS code?
3. Has your company adopted a cybersecurity framework or standard, if so, which one?
4. Which CMMC Level (1-5) does your organization need per current/anticipated DoD contracts? What CMMC Level is your Prime requiring [if applicable] of your company?
5. What CMMC Level can your organization achieve in the short term (within 12-18 months)?
6. Has your organization budgeted for CMMC costs? If yes, approximately how much, if no, why not? Please, choose a range: $0-$25k, $26k-$50k, $51k-$75k, $76k and above.
7. Is your organization concerned that it will not be able to adapt to CMMC required changes? What are your concerns (e.g., leveling up, losing contract)?
8. Do you have major homegrown software systems?
9. Do you think CMMC will help your organization, or the supply chain of which you are a part, mitigate cybersecurity risks?
10. Given your experience, what do you think are the major obstacles your organization will have in adopting CMMC?

Appendix B

CMMC Level 1 – Basic Cyber Hygiene

(*Alt + Left arrow to return to hyperlink location*)

AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.1.002: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.1.003: Verify and control/limit connections to and use of external information systems.
AC.1.004: Control information posted or processed on publicly accessible information systems.
IA.1.076: Identify information system users, processes acting on behalf of users, or devices.
IA.1.077: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
MP.1.118: Sanitize or destroy information system media containing FCI before disposal or release for reuse.
PE.1.131: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
PE.1.132: Escort visitors and monitor visitor activity.
PE.1.133: Maintain audit logs of physical access.
PE.1.134: Control and manage physical access devices.
SC.1.175: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems
SC.1.176: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
SI.1.210: Identify, report, and correct information and information system flaws in a timely manner.
SI.1.211: Provide protection from malicious code at appropriate locations within organizational information systems.
SI.1.212: Update malicious code protection mechanisms when new releases are available.
SI.1.213: Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, and executed.