CMMC IMPLEMENTATION: WHAT IT MEANS FOR SMALL BUSINESSES

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND REGULATIONS

OF THE

COMMITTEE ON SMALL BUSINESS UNITED STATES HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
JUNE 24, 2021

Small Business Committee Document Number 117–021
Available via the GPO Website: www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
44–926 WASHINGTON : 2021

HOUSE COMMITTEE ON SMALL BUSINESS

NYDIA VELÁZQUEZ, New York, *Chairwoman*
JARED GOLDEN, Maine
JASON CROW, Colorado
SHARICE DAVIDS, Kansas
KWEISI MFUME, Maryland
DEAN PHILLIPS, Minnesota
MARIE NEWMAN, Illinois
CAROLYN BOURDEAUX, Georgia
TROY CARTER, Louisiana
JUDY CHU, California
DWIGHT EVANS, Pennsylvania
ANTONIO DELGADO, New York
CHRISSY HOULAHAN, Pennsylvania
ANDY KIM, New Jersey
ANGIE CRAIG, Minnesota
BLAINE LUETKEMEYER, Missouri, *Ranking Member*
ROGER WILLIAMS, Texas
JIM HAGEDORN, Minnesota
PETE STAUBER, Minnesota
DAN MEUSER, Pennsylvania
CLAUDIA TENNEY, New York
ANDREW GARBARINO, New York
YOUNG KIM, California
BETH VAN DUYNE, Texas
BYRON DONALDS, Florida
MARIA SALAZAR, Florida
SCOTT FITZGERALD, Wisconsin

MELISSA JUNG, *Majority Staff Director*
ELLEN HARRINGTON, *Majority Deputy Staff Director*
DAVID PLANNING, *Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

CMMC IMPLEMENTATION: WHAT IT MEANS FOR SMALL BUSINESSES

THURSDAY, JUNE 24, 2021

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
SUBCOMMITTEE ON OVERSIGHT,
INVESTIGATIONS, AND REGULATIONS,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:01 a.m., in Room 2360, Rayburn House Office Building, Hon. Dean Phillips [chairman of the Subcommittee] presiding.

Present: Representatives Phillips, Davids, Evans, Craig, Hagedorn, Meuser, Van Duyne, and Fitzgerald.

Chairman PHILLIPS. All right. Good morning, everybody. I call this meeting to order.

And without objection, the Chair is authorized to declare a recess at any time.

Let me start by saying that the standing House and Committee rules and practice will continue to apply during hybrid proceedings. All members are reminded that they are expected to adhere to these standing rules, including decorum. House regulations require members to be visible through a video connection throughout the proceeding, so please keep your cameras on. And also, please remember to remain muted until you are recognized to minimize background noise. And turn your microphone on when you are recognized, of course.

If you have to participate in another proceeding, please exit this one and log in later. In the event a member encounters technical issues that prevent them from being recognized for their questioning, I will move to the next available member of the same party and I will recognize that member at the next appropriate time slot, provided that they have returned to the proceeding.

For those members and staff physically present in the Committee room today, we will continue to follow the most recent OAP guidance. Masks are no longer required in our meeting spaces for members and staff who have been fully vaccinated. All members and staff who have not been fully vaccinated are still required to wear masks and socially distance. I do hope that we do all our parts to protect each other and our staff.

With that, I will begin with my opening statement. Cyber attacks have the potential to threaten public safety and undermine the American economy and national security. The early months of 2021 have provided harsh reminders of this very fact. Over the past 6 months, hackers and other malicious actors have held an oil pipe-

line for ransom, breached the Nation's largest transit network, and attacked private companies to obtain sensitive customer data.

According to the Council of Economic Advisers, malicious cyber activity has cost the U.S. economy between 57- and $109 billion since 2016. With our society's reliance on technology and digitization growing, there is no doubt that cyber attacks will only become more prevalent moving forward.

Recognizing the urgency of cyber threats, the Department of Defense has taken steps to protect sensitive defense information from attacks aimed at over 300,000 companies that compose the Defense Industrial Base, the DIB. One of these efforts has been the creation of the Cybersecurity Maturity Model Certification. The CMMC is a framework that seeks to improve the protection of different types of sensitive, unclassified information through the implementation of a unifying security standard across the DIB.

The CMMC framework consists of a tiered system with a series of processes and practices at each level. The program was designed based on numerous cybersecurity standards and frameworks. 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 and requirements incorporated a specific CMMC level, only those contractors who have achieved the required CMMC level through the certification process will be eligible for an award.

The need for cybersecurity is unquestionable. It is vital that companies in the DIB become more resilient and prepared for cyber attacks. With that said, the CMMC Initiative has the potential of driving many small businesses out of the Defense Industrial Base, therefore, we must get this right. To that end, it is important to pay attention to the numerous red flags that small businesses have raised about this initiative.

For example, many have a concern about the significant cost associated with CMMC compliance. Guarding against cyber attacks can be cost prohibitive for many small businesses. And firms that seek to abide by CMMC must purchase new hardware and software, replace outdated technical systems, and pay the costs of initial certification and maintenance amongst other expenditures.

Small businesses often run on thin margins as we know, and the cost of CMMC has the potential to leave many small firms in the sector without a chance to compete for government contracts. Many small businesses also don't have the capacity to deal with the complexity of the initiative. Employers at small enterprises often wear many hats and have limited regulatory or compliance resources. This means that independent firms will be forced to turn to outside specialists for help to navigate the program. For many small contractors, this will not be feasible.

According to Department plans, the DOD will implement the CMMC initiative on select contracts between fiscal year 2021 and 2025. In addition, in March, DOD initiated an internal assessment of CMMC partially guided by an effort to manage cybersecurity costs for small businesses. This is a very timely hearing, as it allows us to take a closer look at the program and its implications for small businesses. There is no doubt that contractors working with the DOD must have adequate systems in place to handle

cyber threats. At the same time, we cannot allow the program requirements to drive small businesses out of the defense procurement space.

With that, I would like to yield to the Ranking Member, Ms. Van Duyne, for her opening statement.

Ms. VAN DUYNE. Thank you, Mr. Chairman. We should have compared notes before we gave our opening statements, because I am going to echo many of the sentiments that you just shared.

Just a few short weeks ago, we saw how a malicious ransomware attack perpetuated by foreign actors on the Colonial Pipeline can cause chaos across the entire Eastern Seaboard. And not long after that, another attack shut down one of the leading meat producers in the United States. The potential for profit and opportunity to disrupt U.S. critical infrastructure has invited a number of cyber criminals to target U.S. network vulnerabilities and one of the softest targets to obtain valuable Department of Defense information is through our small contractors.

Recognizing the increased vulnerabilities of small contractors, the DOD initiated new cybersecurity assessment framework, called the Cybersecurity Maturity Model Certification, to assess contractor implementation of cybersecurity requirements. While no one disputes the Federal Government's need to address the growing cybersecurity risks facing our Nation, I am deeply concerned that the CMMC has created yet another hurdle to keep small businesses from competing in the defense marketplace, exactly what we just heard from our Chairman.

A major concern is the cost of compliance. No matter how you look at it, adding stringent cybersecurity requirements will be a costly endeavor for small businesses that are already recovering from a pandemic. With limited resources compared to the competitors in the defense contracting space, small businesses are understandably wary of deploying that capital without assurance that their investment will return in future work.

The Federal Government has already experienced a 38 percent decline in its industrial base for the past decade and measures like this will only exasperate this exodus. Simply put, we need to ensure a competitive contracting environment for small business. This would not only benefit our small employers, but would be a net benefit for our national defense.

I also have major concerns with the rollout of the CMMC for a number of reasons. First, the assessments may be inconsistent and unfair because the new process is being handled by many newly trained assessors. There are also many questions outstanding about how subcontractors will be treated under this new framework.

And, finally, I am worried that small contractors will be shut out of the conversation entirely, and forced to the end of the line.

The fact is that this new process may threaten the livelihood of many small businesses. No assistance, no assessment means no certification, and no certification means no work. Small businesses rightly fear that they won't be given a fair share, left to fend for themselves, as we have too often seen when it comes to sweeping government reforms.

Dealing with cyber threats is an extremely nuanced issue that will require continued collaboration, and while the DOD may have good intentions with the CMMC initiative, we must ensure that the voices of small businesses operating in the Defense Industrial Base are heard and have their concerns addressed. I look forward to hearing the testimony of the witnesses today.

And I yield back.

Chairman PHILLIPS. Thank you, Ms. Van Duyne. The gentlelady yields back.

And I will just take a moment to explain how the hearing will proceed.

Each witness will have 5 minutes to provide a statement and each Committee member will have 5 minutes for questions. Please ensure that your microphone is on when you begin speaking and that you return to mute when you are finished.

With that, I would like to introduce our witnesses.

Our first witness is Mr. Jonathan T. Williams, partner with the law firm of PilieroMazza in Washington, D.C. As Chair of their government contracts group, he counsels companies on a variety of Federal acquisition regulation compliance issues. Mr. Williams is also a member of PilieroMazza's cybersecurity and data privacy team. In this role, Jon works with Federal contractors, particularly those who contract with the DOD, on managing cybersecurity and establishing compliant and effective safeguards. We appreciate your expertise on today's topic.

Our second witness is Mr. Scott Singer, president of CyberNINES with offices in both Wisconsin and Minnesota. Mr. Singer is a retired U.S. Navy captain bringing over 30 years of military experience in both Active Duty and Reserve roles, along with 26 years of industry experience. His company, CyberNINES, is a service-disabled veteran-owned small business, focused on cybersecurity services and a candidate third-party assessment organization for CMMC. We appreciate you as well, Mr. Singer, for your contributions to today's discussion.

Our third witness is Ms. Tina Wilson, founder and Chief Executive Officer of T47 International, located in Upper Marlboro, Maryland. Ms. Wilson is an Air Force veteran, and T47 International is an 8(a) veteran-owned, and women-owned small business, offering a wide range of professional support services to the defense community. We thank you also for sharing your story today.

With that, our Ranking Member, Ms. Van Duyne, will introduce Mr. Dunbar.

Ms. VAN DUYNE. Okay. Hold on just a minute. Thank you very much.

I would like to welcome our final witness, Mr. Michael Dunbar. Mr. Dunbar is the president of Ryzhka International, a service-disabled, veteran-owned small business founded in May of 2011, and a HUBZone certified firm as of February of 2014. They have lubricants and fuel oil to government, commercial, and maritime clients worldwide, and proudly provide 100 percent American-made products. From its initial founding to today, the company has grown from one to six employees and successfully serves clients ranging from the U.S. Army Corps of Engineers, the Department of Veterans Affairs, the U.S. Navy and Coast Guard, the National Oce-

anic and Atmospheric Administration, various shipyards in many of the dredging community.

Ryzhka International has been the proud recipient of several awards. This is the Department of Defense's award for support of the Guard and Reserve. And in addition to its businesses, the company's secondary mission is to provide gainful employment opportunities to qualified individuals from disadvantaged segments of society, such as minorities, women, people with disabilities, and veterans.

Chairman PHILLIPS. And we will begin with Mr. Williams—oh, I am sorry.

Ms. VAN DUYNE. Sorry. You are good. You are good. The secondary focus is no surprise considering Mr. Dunbar's own military service in the U.S. Navy Nuclear Power program and its status as a service-disabled veteran. After his military service, Mr. Dunbar went on to spend the summer working on the solid rocket boosters for National Aeronautics and Space Administration's space shuttle.

Following that summer, he attended the University of Utah, went on to have a successful career as an executive in the biotech industry, and afterwards, started his own company. Mr. Dunbar will be speaking today on behalf of the HUBZone Contractors National Council, which is a nonprofit trade association advocating for policies bringing opportunities to HUBZone certified small businesses and the economically disadvantaged communities in which these companies are based.

Mr. Dunbar, thank you for your participation today. We look forward to hearing your testimony.

I yield back.

Chairman PHILLIPS. Thank you, Ms. Van Duyne. The gentlelady yields back.

Sorry, Mr. Dunbar. My bio is about one sentence long, so I am not accustomed to two pages.

With that, we are going to recognize Mr. Williams for 5 minutes for your opening statement. Mr. Williams.

STATEMENTS OF JONATHAN T. WILLIAMS, PARTNER, PILIEROMAZZA PLLC; SCOTT SINGER, PRESIDENT, CYBERNINES; TINA WILSON, CHIEF EXECUTIVE OFFICER, T47 INTERNATIONAL, INC.; AND MICHAEL DUNBAR, PRESIDENT, RYZHKA INTERNATIONAL LLC, TESTIFYING ON BEHALF OF THE HUBZONE CONTRACTORS NATIONAL COUNCIL

STATEMENT OF JONATHAN T. WILLIAMS

Mr. WILLIAMS. Good morning, Chairman Phillips, and other distinguished members of the Subcommittee. My name is Jonathan Williams, and I am a partner with the law firm PilieroMazza, which represents government contractors. Many of our clients are small businesses that work with the Department of Defense as prime contractors and subcontractors. It is an honor to participate in this hearing on DOD Cybersecurity Maturity Model Certification to share my perspective on the CMMC Initiative.

DOD's focus on cybersecurity has been steadily building for many years, with measures ranging from implementation of new regulations and contract clauses to the elevation of cybersecurity as the

fourth pillar of DOD's acquisition planning. DOD has left no doubt about the importance it has placed on enhancing cybersecurity for the Defense Industrial Base, and with good reason, as recent events like the pipeline shutdown demonstrate.

CMMC marks a significant change in DOD's evolving approach to cybersecurity. With CMMC, contractors will no longer be allowed to use the honor system by self-certifying their cybersecurity. Instead, contractors will have to apply for certification from a third-party assessor. These so-called C3PAOs will evaluate the contractor's cybersecurity against established benchmarks and decide whether to certify the contractor in one of five levels.

The lowest level of CMMC is level one, which requires the fewest and most basic cybersecurity measures. The level one requirements are things all businesses should be doing, like spam filters and antivirus software. The cost and complexity of the requirements increases significantly at the higher levels of CMMC.

DOD has said it intends to start requiring CMMC on a few contracts this fiscal year with that number increasing steadily over the next several years until fiscal year 2026, when all DOD contractors will be required to have CMMC.

However, the implementation schedule has slipped a few times already and remains in flux. Approximately 2 years into the CMMC Initiative, many practical questions that small businesses are asking remains unanswered. These are basic questions like, when will I need CMMC? How much will it cost? What level do I need? And how do I get it?

Many small businesses will not be able to adequately prepare for CMMC until these questions are answered. For example, DOD estimates that most small businesses will only need level one; however, that is not guaranteed. DOD agencies are more likely to require at least level three for many of their contracts, and prime contractors may flow down the same level to their subcontractors.

Given the substantial difference in cost and technological know-how between level one and level three, many small businesses will be unable to compete if more than a level one is required. From my discussions with the small businesses we represent, I have several suggestions for how to make the CMMC Initiative more manageable for small businesses, including the SBA and DOD mentor-protege programs should be utilized to ensure that mentors provide small businesses with resources and guidance to obtain CMMC.

Joint ventures, a popular tool for small businesses to pursue government work, should not be required to have CMMC when the member companies are certified. C3PAOs should be required to fast-track CMMC applications when the applicant is a small business that is in line for award of a contract.

DOD contract clauses should prohibit prime contractors from imposing a more stringent level of CMMC on a subcontractor than is necessary based on the scope of the subcontract.

And finally, DOD and prime contractors should explore alternative ways to give small businesses access to sensitive information that will enable more small businesses to participate on DOD contracts with a level one certification.

In closing, I believe the CMMC Initiative appropriately aims to improve our Nation's cybersecurity posture. I do not think small

businesses would debate the importance of cybersecurity, or that doing business with the Federal Government is a privilege that requires investments in compliance and infrastructure.

At the same time, the worthy goals of the CMMC Initiative must be calibrated to avoid creating an unnecessarily high barrier to entry for small businesses, which are the engine of our economy and critical partners with the Federal Government for innovation and provision of many necessary services and supplies.

This concludes my testimony. Thank you, again, for the opportunity to appear before you today.

Chairman PHILLIPS. Thank you, Mr. Williams. A perfect 5 minutes at that. We appreciate it.

Now we recognize Mr. Singer for 5 minutes.

STATEMENT OF SCOTT SINGER

Mr. SINGER. Thank you, Representative Phillips, Ranking Member Representative Van Duyne, and members of the Subcommittee, for inviting me to testify this morning. I look forward to providing information that will help ensure we have a secure Defense Industrial Base and find cost-effective solutions to allow small business to fully comply with CMMC.

My name is Scott Singer, and I am the owner and president of CyberNINES. CyberNINES was founded only in June of 2020; however, thanks to the interim final rule released on November 30, 2020, we have been really busy. And I have done assessments in the districts of some of the members of this Subcommittee. Small businesses do not have purchasing or IT departments. They do not have compliance or regulatory departments. We need to make this easier for them. Primes, certified third-party assessors, registered provider organizations, all can assist these small businesses get compliant and reduce the complexity for them.

Having a program where the primes take a strong guiding hand of their supply chain is critical to maintaining these small businesses as DOD suppliers. Of the last 33 basic assessments CyberNINES has conducted, the average compliance score was minus 105. Plus 110 is perfect. We have found that on average, they are about only 34 percent of the way toward meeting all the risk controls. Cost models put forth by the government assume that companies are much further along on this journey, and they actually should be by this point.

Assuming full compliance to NIST, the DOD has put out that this will cost $26,000 to complete the 20 additional practices followed by an additional $29,000 to be assessed by a C3PAO. As discussed above, small businesses that we have assessed are only partway there, and we have come up with costs more to the tune of about $130,000 for these businesses to be able to be compliant.

Last week, I conducted a basic assessment of a small manufacturer in Minnesota. They had only six employees, one small manufacturing space with three machines, and they do excellent innovative work. I spent a good majority of my time doing the assessment actually from the owner's house. This year, he expects to make 875K in revenue. My estimate is that if he wants to stay a DOD contractor, he will have to spend 10 percent of his revenue over the next 3 years alone on getting compliant.

Small businesses have been directed to add their allowable costs to get compliant to their indirect rates. Most don't do cost reimbursement contracting for DOD. Moreover, market factors around competition for orders will require them to compete and lower prices. Established contractors will be more likely to be able to provide a lower bid and win the order from the prime. There should be a process separate from the competitive marketplace to allow small businesses to get paid for the reasonable, necessary, and allowable cyber compliance expenses.

Companies further ahead should not be penalized and be able to recoup their past expenses, too. In addition to the difficulty small businesses have funding this effort, there are bottlenecks for getting enough assessors. In doing the math, I just don't see how—and this is my opinion—we can get enough C3PAOs and assessors through the process to assess 300,000 DIB companies by October 1, 2025. I saw one estimate that we would need over 8,000 assessment team members working full-time from today on to make this happen.

To get more C3PAOs through the process, I recommend there be a relaxation for the initial C3PAOs. Assess candidate C3PAOs to maturity level one or two now, and then require level three in the future. The requirement for tier three background investigations for assessment and support staff creates another bottleneck. I would recommend allowing an interim clearance process for that.

In conclusion, the majority of the 300,000 contractors in the DIB are small businesses. Without monetary support and clear regulatory guidance, the DOD will lose small businesses as they will look to find business in the commercial sector. A balance must be struck between risk and cost. Too much cost, we lose suppliers; too much risk, and we hurt our national security.

Thank you for allowing me to testify, and I look forward to your questions.

Chairman PHILLIPS. Thank you, Mr. Singer. And now we recognize Ms. Wilson for 5 minutes.

STATEMENT OF TINA WILSON

Ms. WILSON. Chairman Phillips, Ranking Member Van Duyne, and members of the Subcommittee, thank you for the invitation to testify today. I am Tina Wilson, CEO, T47 International, and I am honored to have the opportunity to provide some insight regarding the implementation of DOD CMMC Initiative.

As a business owner with over 260 employees located in 28 States and overseas, T47 provides a variety of staffing services from budget and finance, janitorial, inventory management, aircraft tools, maintenance to mail room, and nonclinical medical and dental case managers. The diversity of services offered puts me in a unique position to provide a different perspective regarding this subject.

As CMMC standards continue to be developed and incorporated into contract agreements and modifications, it is essential that the Small Business Committee be aware of the policy impact. If the CMMC standards are not clearly communicated and monitored for fraud, the financial ramifications to the over 300,000 Defense In-

dustrial Base of contractors, and specifically to the small business community, could be devastating.

Based on this statement, I will cover three main subject areas of concern and offer recommendations.

Cost to secure CMMC. As of today there is no set cost to obtain CMMC. The CMMC accreditation body has stated that the marketplace will need to define the cost, which leaves it wide-open for interpretation what this cost will be. Whether it is a tiered cost based on the size of the business, or a set cost regardless of the size, there will be initial and sustained cost that will impact small businesses' ability to secure the certification.

A similar certification offered by the International Organization for Standardization, ISO, is standard 27,000, which is information technology and focuses on security for any kind of digital information. This certification costs between 28- to $35,000 to obtain, and takes approximately 6 to 8 months to implement. This is a tremendous cost burden to add to a very tight budget for most small businesses.

Cost of not having CMMC. While unknown as of today, what has been communicated to the entire Defense Industrial Base is that if you don't have CMMC at the basic level, you will not be eligible for a Federal contract. Many small businesses may not even be aware this new requirement and failure to obtain certification means ending contract work as a service provider to the DOD.

Additionally, as the prime contractor, it will be our responsibility to flow down the requirements to our subcontractors. If the subcontractor does not have certification, we would be required to end subcontract agreements to remain compliant with the DOD CMMC standards.

Audit imposters. I raise this subject as an awareness to inform the Subcommittee. When the DOD presented the CMMC as the new way of life for all businesses within the Defense Industrial Base in the summer of 2019, many business owners asked a lot of questions of why? Who will conduct the implementation and audit? How much? When will it happen? Implications, or if you do not have it, and many more questions.

Before the CMMC accreditation body was formed in the latter part of 2019, audit imposters with no training and not accredited, start advertising that they will certify your company as cyber compliant for thousands of dollars to get a company ready. For many small businesses that are just now hearing about this standard, may in a moment of panic and fear of losing their government contract, may fall prey to an audit imposter.

As I close, I recommend that the Subcommittee members closely monitor this very important implementation of CMMC Initiative. While I know there are so many other issues to focus on, CMMC has ramifications that reach far beyond what we can realize at this moment.

It is important that, one, cost is articulated clearly to reduce price gauging and to allow the small businesses to plan; number two, a balanced cost approach that does not reduce small business participation in the Federal marketplace; number three, DOD continues to work closely with various advocacy groups to ensure that the Defense Industrial Base contractors, known at the Office of

Small Business, is aware of this implication to this new initiative; and four, DOD and the Office of Small Business start as soon as possible to put various roadblocks in place to reduce the number of audit imposters.

Thank you for your time in addressing this very important subject that impacts thousands of small businesses that do business with the Department of Defense.

Chairman PHILLIPS. Thank you, Ms. Wilson.

And now I recognize Mr. Dunbar for 5 minutes.

STATEMENT OF MICHAEL DUNBAR

Mr. DUNBAR. Chair Phillips, Ranking Member Van Duyne, and members of the Subcommittee, thank you for the opportunity to testify before you today. My name is Michael Dunbar, and I am the president of Ryzhka International, located in Pompano Beach, Florida.

Ryzhka International provides lubricants, fuel oil in bulk quantities, package quantities to the Federal Government, commercial maritime industries. I am a proud service-disabled, veteran-owned small business, as well as a HUBZone certified small business.

I am testifying today on behalf of the HUBZone Contractors National Council, a nonprofit trade association providing information and support for companies and professionals interested in the Small Business Administration's HUBZone program. We would like to thank the Committee for its commitment to small business and for advancing policies that support small businesses doing business with the Federal Government.

In a recent hearing, Deputy Assistant Secretary of Defense of Industrial Policy, Jesse Salazar, said it best: The Department's approach to cybersecurity must balance the need for accountability with the recognition of the challenges facing small businesses.

Small businesses understand the importance of cybersecurity, and the very real threats facing their companies. We are not looking for a way to opt out or ignore this problem. We want to secure our companies. According to the DOD's contracting data, 74 percent of the Defense Industrial Base are small businesses. These contractors are critical to the government, and are not a group that can be ignored.

The Federal Government has long identified the need to safeguard sensitive information and understands that cybersecurity is dynamic issue. Small businesses, however, are experts on the goods and services they provide. We do our best to focus on supplying a product, making a profit, and retaining employees. Most small businesses are not IT professionals. We are not cybersecurity specialists either. I am—right here is the assessment guide. This is for cybersecurity CMMC model level three. It is full of stuff I have no idea and don't understand. I have to hire somebody to figure this out.

The initial cost for me to start my business was less than $1,000. The cost to start a new government-focused business with this, 10,000, 100,000; we really don't know. Access to capital can be a very challenging issue for small businesses, and we have to use significant capital now to become CMMC certified.

The segments hurt most are the segments that can least afford it. The Federal Government already has challenges meeting those goals. If we reduce the number of companies that qualify, you also reduce opportunity for people to start up new businesses in those sectors.

The council makes the following recommendations to improve the rollout of CMMC, and maintain a strong industrial base. Increased cost transparency and put guardrails on rising compliance costs for small business. One of the biggest frustrations for small business throughout the rollout has been cost transparency. Some small businesses have estimated costs in excess of $100,000 to prepare for level three certification. That doesn't include the assessment costs. I have heard of assessment costs already estimated at above $150,000 for a 50-person company.

Establish clear communication on CMMC efforts. A lack of transparency, clear, consistent communication by the DOD, and the rollout of CMMC and its implementation by the CMMC accreditation body has been concerning. The council suggests putting together a more clear, consistent delivery of information through a central government platform or website.

Streamline new and existing standards for contractors. The Federal Government lacks unified cybersecurity standards across all agencies. The council encourages the DOD to work closely with industry, particularly small businesses, to streamline these requirements allowing companies to have a plan of action and milestones after a CMMC assessment would help these burdens.

Create a system for oversight and equitable rollout. Many small businesses worry that they will be put at the back of the line and face massive delays as companies serve the subcontractors, and equitable rollout is important to these companies as well.

In conclusion, the Federal Government has a long and complex history of governing cybersecurity regulations and compliance with its contractors. A streamlined approach needs to be taken for contractors to navigate all of these standards and system successfully.

Thank you for the opportunity to testify today, and I look forward to your questions.

Chairman PHILLIPS. Thank you, Mr. Dunbar, and to all of our witnesses for being with us today and we appreciate your testimony on the CMMC Initiative.

I will begin the hearing now by recognizing myself for 5 minutes. I will start with Mr. Williams.

I think we all understand the importance of cybersecurity, and ensuring that the most vulnerable small businesses in the DIB supply chain are protected. However, it is clear that the cost of CMMC could be terribly burdensome for small businesses. So how should we be looking at this? How can we strike the right balance between enhancing cybersecurity, and ensuring that small businesses can participate in DOD acquisitions?

Mr. WILLIAMS. Yes. Excellent question. Thank you. I think one of my top suggestions there is to try to make good on DOD's estimate that most small businesses will only need level one. As I said in my testimony, that is not guaranteed, but if we can keep as many small businesses as possible at level one, that will strike the right balance between ensuring that these small businesses have

at least the basic cybersecurity protections in place, but will allow them to avoid, as Mr. Dunbar said, the significant additional costs when you go from a level one to a level three.

And I think managing the level one versus level three distinction is probably one of the most critical ways to keep the cost down for small businesses. That could be done through flow-down protections. Make sure that primes are not flowing down higher than level one if their subcontractors only need level one. And I would like to see more flexible approaches where the small businesses don't need to take the controlled unclassified information into their own network, because that is what then causes the jump from level one to level three.

Let's look at ways that either the DOD and their own systems, or the prime contractors and their own systems, can maintain this information, and let's maybe be more creative and flexible in how we allow small businesses to participate on those programs without having to take that information into their network, and then cause them to have to go up to a level three.

Chairman PHILLIPS. Appreciate that. Are there any funding streams of which you are aware that can help small businesses with the costs of CMMC? And if there is anything that Congress, DOD, or even SBA could do to help in that regard, no matter how significant the expenses might be?

Mr. WILLIAMS. I am not aware of specifically targeted funding stream at CMMC. I think it would be a fantastic idea if there was the wherewithal for a grant program for small businesses to help them on their way with the upfront investments needed for CMMC.

The larger small businesses will be able to make that investment and get it on the back end when they are paid on their contracts with the government, but for the smaller firms, even the several thousand dollars of the investment needed for a level one might be too difficult to make upfront.

And I think the existing mentor-protege programs, as I mentioned, those are fantastic programs. They work very well in many respects at the SBA and DOD for small businesses and large businesses. There are a lot of incentives that large business mentors get from participating in those programs.

We could be clearer, more well-defined that mentors, when they are permitted to access those programs, have to ensure that one of the things they are doing for their proteges is to provide financial resources and technical assistance to ensure their proteges are ready for CMMC.

Chairman PHILLIPS. Thank you very much.

Ms. Wilson, I would love to hear from you about your experience. How were you made aware of CMMC? How difficult is it for you and T47 to understand, and do you envision having to engage a consultant or specialist to help you navigate it?

Ms. WILSON. Sure. Thank you for the question. I learned about CMMC when attending a DISA Industry Day in 2019 up in Baltimore. I understand completely how it works and, you know, from a broader perspective, but, you know, protecting supply chain, intelligence, assets, IT infrastructure and, you know, things that matter to protect in our Nation.

And for T47, the critical part is, we have to secure a specialist, which I have already engaged, because it is very complex. And for someone that is non-IT like myself—I am a business owner. I know how to go get contracts and build a company, but to build an IT infrastructure that impacts a lot of employees and be able to maintain it and go into other secured areas, it is a challenge.

So to actually have an expert to help us is going to be critical, and I have engaged in that process already.

Chairman PHILLIPS. Thank you very much. My time is expired, and now I recognize the Ranking Member, Ms. Van Duyne, for 5 minutes.

Ms. VAN DUYNE. Thank you very much. Mr. Dunbar, okay, hold that up one more time. You need two hands. That is—I mean, I completely understand your frustration right now. Do you believe that the CMMC duplicates any of the multiple standards in cybersecurity programs that currently exist? Do you find that there is a bunch of stuff that is already existing right now that is in that book that you are going to have to do more of? And is there a way to further streamline these disparate processes?

Mr. DUNBAR. Thank you very much for the question here. From what I understand—and I am not a technical expert, so I will answer from a layman's perspective—CMMC added, I believe, 20 additional items to NIST 800-171, which is currently the law of the land and what exists today. So what is being projected to be our new standard is built on an existing standard, and part of me questions why we had to go so much further.

The reasoning behind putting CMMC in place, part of it was because we were doing self-assessments before for companies instead of having a third-party assessment. Why could they not institute some part of third-party assessment to an existing standard? Why create a whole new standard that people have to learn and understand to begin with?

And I didn't have to deal with the first standard because most of my business is what they call is called COTS, which is Commerical-Off-The-Shelf products; however, fuel recently, as we just saw with Colonial Pipeline, has become a very critical item. Is supplying fuel by truck, by whatever method all of a sudden going to become a CMMC level four like the infrastructure piece of it might potentially need to be? That is going to impact a significant number of small businesses like mine.

So by adding these additional items, we ask our question as to why, and how do we streamline this? I have in place security right now that covers 77 of the NIST items—covers 77 of the CMMC items, but covers 90 percent of the risk. So is that additional cost-benefit, and we are talking 80 to $100,000 of additional cost to get that other 10 percent realistic for small business?

Ms. VAN DUYNE. I am concerned that the critical information about CMMC is being conveyed in a conflicting and potentially informal manner. What are small businesses currently going to seek information or guidance on CMMC? Where are you going to find more information? And then, what would be the ideal method or platform of communication from the DOD to the contracting community? How can we make it easier?

Mr. DUNBAR. The main place that we have been receiving information tends to be LinkedIn. We have had members of DOD communicating directly through LinkedIn, members of the CMMC board communicating through LinkedIn. That tends to be the largest location or community of folks getting information on this program. We get very little from DOD directly. They have had some town halls that they call it. You don't really get much notice, if any.

Just the other day was mentioned a project spectrum, I believe it is called, that I had never heard of, that was put in place, it looks like some time in 2020. Most small businesses are unaware of this as well, and this is supposed to help us somehow, it is a DOD program, but we are not even aware of it.

Ms. VAN DUYNE. Your being sent to a website is probably not going to help you?

Mr. DUNBAR. Correct. And that is just—there is no consistent method or message coming out from DOD on where to get things. Even if you go to the CMMC-AB frequently-asked-questions page, sometimes they say Oh, that is a DOD responsibility, and that has been a lot of the kickback is pointing fingers between the CMMC-AB and DOD saying, Well, they are responsible for X; they are responsible for Y.

Ms. VAN DUYNE. Specifically for the small business community, I didn't mean to cut you off, if you had anything else to add.

Mr. DUNBAR. No, ma'am.

Ms. VAN DUYNE. Specifically for the small business community, and I hate to add another agency in here, but do you see a role that SBA could possibly play in helping to be an intermediary between the three?

Mr. DUNBAR. I definitely—there should be a role for the SBA in here. I don't feel that the SBA has been able to be involved. I feel that the DOD has sidelined them, at least in my opinion, in the same manner that I think a lot of small businesses have been ignored when we have raised questions or raised issues. And that has basically been kept to a very small group of people that are running all of this, and then we get told later on, Here is what is happening.

Ms. VAN DUYNE. Thank you very much.

I yield back.

Chairman PHILLIPS. The gentlelady's time is expired.

And now I recognize the gentleman from Pennsylvania, Mr. Evans, for 5 minutes.

Mr. EVANS. Thank you, Mr. Chairman. I would like to ask a question to Ms. Wilson. Small businesses are frequently targeted by cyber criminals. What would the ideal situation be for you in terms of the Department of Defense ensuring that cybersecurity taken care of its small business base?

Ms. WILSON. Thank you so much, sir. I think one simple solution to offer, and it could be reasonable cost and possibly free. It is the offer of maybe cyber tools that are already approved by DOD to the small business community as a first line of defense. It could be offered up from the CMMC level one up to possibly level two. And then, at least this way, DOD has a level of comfort to say, Okay, at least we have some tool out there now, it is up to the mar-

ketplace, the small business community to go out and secure additional certification, if necessary, to ensure that, you know, at least we are taken care of, and that shows an effort that the DOD cares. That is a critical part. We just need to know that DOD is here to help you.

Mr. EVANS. I would like to follow up. For many small business, cybersecurity certification is just one of the many requirements of certification they need to comply with as part of being a defense contract. Can you mention just a few of the other certifications you have to comply with, and how does the cybersecurity certification compare to other certification in terms of its levels of burdens?

Ms. WILSON. Sure, sir. So for T47, we have actually invested in securing the ISO certifications, three certifications. We are doing that currently. That is a very costly investment. We will also have the SBA 8(a) certification that is due annually. And because of our size now, we now must incur additional cost for audits that are necessary to keep the certification.

We have the woman-owned small business certification, and then as a clear facility, we have the defense counterintelligence security certifications as well to keep our clearance.

So, in comparison to all those other certifications was just a small list for us. To be perfectly clear and frank with you, the CMMC has been the most challenging, because it is just a lack of not understanding exactly what is needed, and it is a cost that is involved. There is no transparent cost set aside for, like, small business mid or large.

And I know this is a new initiative because any time you roll out a new policy, there is always going to be bumps in the road, but at the same token, there needs to be more of a clear communication from DOD, and those that are managing this process on what it is going to take for small businesses, or all businesses to have the certifications necessary.

And that is going to take a concerted effort for everyone to understand. CMMC, to be quite honest with you, it is new, but it is a challenge. And it must be worked out pretty quick because you are going to start rolling these things out into contracts, and the fear could be real once it starts happening.

Mr. EVANS. I thank you.

And I yield back the balance of my time.

Thank you, Mr. Chairman.

Chairman PHILLIPS. The gentleman yields back.

And now I recognize the Ranking Member of the Subcommittee for Underserved, Agricultural, and Rural Business Development, Mr. Hagedorn of Minnesota for 5 minutes.

Mr. HAGEDORN. Mr. Chairman, thank you for that, Ranking Member Van Duyne. It is good to be with you today. Thanks to the witnesses. This seems to be one of these issues, and even the big agencies the Federal Government want to impose a lot of things on small businesses that they themselves don't handle appropriately.

It doesn't take—you don't have to think too long and hard to realize that the DOD has lost technology outright, giving it away in some cases, our Federal Government, to China. Economic technology, of course, gets lost a lot by big companies. OPM went and took 25 million records of Federal employees. I was one of those

folks that they stole from during the Obama administration, and now they come along and say, Well, if you want to do business with us, you have to go through a bunch of gyrations, spend a bunch of money, and some of it, it seems, could be reasonable.

You look at recently, we had some issues with, obviously—and these things are very important. We had a big meat packing company that does 25 percent of the beef in the United States; have a pork manufacturing plant in Worthington, Minnesota, where I represent, they went down and you see how critical things can be. We can lose our food supply and everything else in the blink of an eye, but Mr. Dunbar, I think—wouldn't it make more sense if the Federal Government just imposed some reasonable standard and said if you want to do business with us, you got to try to do everything possible in order to make sure there is security here, and that you protect these digital ways that you do business? I mean, rather than have you go through all these hoops. I mean, you say it costs up to $100,000, it doesn't seem reasonable to me.

Mr. DUNBAR. Thank you, sir, for the question. Yes, I agree. I think the keyword there is the definition of reasonable. I believe the DOD believes that their numbers and that their requirements are reasonable. Small businesses would probably disagree with that when you have a company like mine of six people that has to spend $100,000 to comply with something.

There are, as I mentioned, standards out there currently that are being used every day. I mean, right now, a small business—you walk into a small business and we hear advertisements on TV and such saying, We have got your security, Have your internet service through us, we got you covered. Well, that is what a small business thinks. Okay. They got our security for us. No problem. Then we see something like this and say, Well, we really don't have security, do we? We need something in between those two items.

My security that I currently have in place is, as I mentioned, covers 77 of the items that are being requested in 90 percent of the problems, and it is costing me about $15,000 a year to $20,000 a year to do that. I could get away with a little bit less, but I have insurance and other things on it that get tossed into there to cover in case I get hacked.

So there are standards out there that could cover reasonably well what we are all looking for, and meet a level, I think, that would provide security for anything but the greatest items out there. As was mentioned by Mr. Williams, having access into a system provided for us for companies that don't need to take something or machine it, but actually just need that data and that information can go into the government system sort of like the National Guard does. They have their little wall garden, we call it. A member of the National Guard can go in, get their CUI information in there, go out, be it their VPN, and now they have all the information that they need, and it has been in a secure environment.

Mr. HAGEDORN. So I worked a little bit in the Treasury Department, and I have seen bureaucracies in action and usually the bureaucrats come up with lots of ideas in order to make sure that if something goes wrong they can, as you say, point the finger at somebody else. And I see a lot of that here. I see a lot of expense

being pushed along to you, and just because if something goes wrong, they don't want to be blamed for it.

And I think, you know, it is kind of telling when government comes up with these ideas here, we are going to put this regulation on you, we are going to make you do all these types of things, and oh, it is going to cost some money so, well, now let's go find funding streams in order to help you pay for that. I mean, we see this all day long.

I think a reasonable standard would make sense. Most businesses, even the big ones, have issues here. They all need to do better in compliance and I think that people can figure that out. So thanks very much, by the way, for your service to the country and you had a very impressive resume. Took our Ranking Member an extra shot at it just to get it out.

Thanks very much.

Mr. DUNBAR. Thank you, sir.

Chairman PHILLIPS. The gentleman yields back.

And now we recognize the Ranking Member of the Subcommittee on Economic Growth, Tax, and Capital Access, Mr. Meuser, for 5 minutes.

Mr. MEUSER. Well, thank you, Mr. Chairman. Thank the Ranking Member very much for holding this hearing. Thank you to the witnesses as well. So there are reports—we all know that cybersecurity is clearly an issue. Reports are, that I have reviewed, that 6 percent of U.S. military and aerospace contractors reported data breaches between 2016 and 2018. Ransomware attacks are up over 100 percent in 2020. All industries, by the way. That is for all industries. So it is a concern.

DOD, however, seems to have created the CMMC mandates that are a major concern to all small businesses and contractors certainly sitting here, and in my district. In fact, it seems that some of the focus on compliance with these mandates is even truncating your actual ability to focus on actual cybersecurity. And as being in business for a lot of years, I understand that. These mandates coming from Washington, in this case the Department of Defense, don't take what your business about fully into consideration. How could they possibly, right? I mean, it is a one-size-fits-all approach.

So, I am definitely not happy to hear that the Department of Defense is also not offering forums to have this discussion with you, right? Perhaps in a hearing maybe we can do that or create access so they can better understand your concerns. And, again, I have DOD suppliers in my district that have already, just in the last couple of years, spent tens of thousands of dollars living up to these requirements and trying to achieve them. And meanwhile, they don't necessarily even know what level they are at, and they are very concerned, even their midlevel suppliers of those who are supplying them, being able to maintain those costs. Everything that you are discussing sharing here.

So Mr. Dunbar, I will just ask you this: Level one, we are talking about level one here, what is—do we have the Department of Defense's feedback on if level one is satisfactory, and for how long it will be because I know they are trying to roll into this with a—in a managed way over the next several years, right?

So what do they say about you and suppliers that you know about maintaining level one at this point?

Mr. DUNBAR. Well, I think you reached part of the problem, is we are not really hearing a lot. We have got some estimated dollars and some numbers out there tossed around to level one, and yet how long is it supposed to last, any of the real detail on it? We don't get a lot of that. As you mentioned, the technology, is that going to keep up, or are we going to keep chasing technology as we go along, and, therefore, chasing more regulations and more rules that we have to get reassessed for along the way which are just going to continue to increase costs?

Mr. MEUSER. Speaking of cost, what is the cost difference, would you estimate, from level one, which many are saying here they believe would secure your systems and your companies versus say level three? Can you put a number on that?

Mr. DUNBAR. Easily ten- to twenty-fold.

Mr. MEUSER. Wow. Okay. And how much more secure would it be from level one to level three?

Mr. DUNBAR. I don't really know specifically from a level one to level three how much more secure it would be. I know from where I am currently, and what I am paying for the setup I have, which is a pretty secure setup, according to—the person who handles my security is actually a past director at DCISC for the Department of Defense, so he is the one who set mine up, and he is the one who said that we have 77 of the 120 controls and have 90 to 95 percent of the issues.

So he believes for very small companies that you could be looking at, you know, 5 to 10,000 a year maybe for your costs instead of, you know, having to reach up to this level and that same company could be at hundred-plus thousand dollars a year.

Mr. MEUSER. Well, I think we can conclude that these measures are overly harsh and we do need to create a forum to have this discussion with DOD so we can work this out.

I yield back, Mr. Chairman.

Chairman PHILLIPS. The gentleman yields back.

And that completes our first round of questioning. So, therefore, I will recognize myself for another 5 minutes.

Mr. Singer, while companies like yours in the pipeline become accredited C3PAOs, there is a long ways to go until we have a substantial amount of them. So how likely is full implementation of CMMC by 2026, if there is a lack of assessors?

Mr. Singer?

Mr. SINGER. I forgot to unmute.

Thanks for the question, sir.

I think it is very difficult to get there with the current progress we are making. We have a hundred provisional assessors at this time, and we have two C3PAOs already through the process from doing a DOD assessment. And, by the way, the third-party assessors are going through that level three assessment, so we have to meet the 130 different practices.

So I think it is very difficult. The timeline is very stretched. As I had said in my testimony, I think we need more than 8,000 assessment team members to even make this happen, and that would be starting from today. So the math just doesn't work. I believe

that there does need to be some flexibility in how we are rolling this out to the third-party assessors, and we need to have some—you know, if we are going to try and meet that deadline, there needs to be quite a bit more flexibility by the DOD in trying to ramp this up and move this out.

I also feel pretty strongly that not everybody, as we have talked about before, needs to be at level three. If you are a part component maker, a small business, and you are doing, you know, special processes like coatings, painting, and somebody—a prime flows down a drawing to you and tells you, Put the label plate here on this, you know, equipment, all of a sudden you have now had to hit level three.

So there is some work here that needs to be done on understanding the risk truly to the supply chain, and maybe a single part maker of a bracket doesn't need to be level three, but somebody that is making sub assemblies and more complex parts does need to be.

So that would be my answer.

Chairman PHILLIPS. Thank you, sir.

And, Mr. Williams, while CMMC is a DOD initiative, we are beginning to see it in other solicitations, particularly for government-wide contracts like GSA's 8(a) STARS III contract. So how concerned should small businesses be of the CMMC Initiative being adopted by civilian agencies and becoming a de facto baseline for doing business with the Federal Government?

Mr. WILLIAMS. Yes, I think that is certainly a possibility. You know, the rollout with CMMC at DOD has experienced challenges, as we have been covering in today's hearing, and I think it remains to be seen if they will hit the target of 2026 as Mr. Singer just said. I would view what is happening at DOD as a trial balloon. And if it went well at DOD, which certainly is an open question at this point, I wouldn't be surprised at all if it is expanded beyond DOD to all of government.

Chairman PHILLIPS. All right. Thank you, sir.

And with that, I will now yield to Ms. Van Duyne for 5 minutes.

Ms. VAN DUYNE. Thank you very much.

Mr. Singer, I appreciate your testimony here today. I just have a couple of questions.

What is the penalty or the outcome for a small business that can't comply with the requirements?

Mr. SINGER. Today, the penalty is that you are out of doing business with the DOD, period.

Ms. VAN DUYNE. Okay. I mean, that is—I am seeing Mr. Dunbar shake his head as well.

So I am going to ask actually the whole panel, can you point to one or two concrete things that we can do to make understanding these flow-down requirements easier for small business? Mr. Hagedorn had a great point, well, yes, we could just define reasonable and move forward from there. Can we be a little bit more specific on what you would need?

And, Mr. Singer, we will go ahead and start with you.

Mr. SINGER. Sure. Thanks for the question.

I think it is really—I think the primes really need to step up and play a bigger role here. They have the resources and the teams,

and they have done a lot of the background work on understanding what is required. And instead of just sending out a rep and certs or a letter to a small business saying you need to post a score in the supplier performance risk system, I think there needs to be more support and help for them and more of a guiding kind of process program that they implement for their whole supply chain to help them get compliant.

Ms. VAN DUYNE. Ms. Wilson, do you have anything to add?

Ms. WILSON. Yes, ma'am.

To ensure that everyone is on the same page and have the same information. What we have right now is pockets of information going to various individuals, like I just heard from Mr. Dunbar, said most of the information is being flowed through LinkedIn. Some companies have LinkedIn and some companies do not. There needs to be concerted effort of communicating what the standards will be, what the costs will be across all industry, and filter down to the small business, and maybe a regional approach to be able to help understand that CMMC is here to stay, take away the fear, but communicate clearly what it really means to have this certification.

Ms. VAN DUYNE. Awesome. Thank you.

Mr. Williams?

Mr. WILLIAMS. Thank you.

Yes, I would like to make two points. First to address the comment about flow down. The interim DFARS clause for CMMC which was issued late last year directs prime contractors to flow down the CMMC level that is appropriate for the information that is being flowed down to the subcontractor. That gives a lot of discretion to the prime contractor to decide what is appropriate. I would like to see the final DFARS clause for CMMC prohibit prime contractors from flowing down a higher level than is absolutely necessary based on the information that is being provided to the subcontractor.

And the second point I would like to make about the information that is being disseminated to the small business community, my experience has been that there have been town halls, as Mr. Dunbar mentioned, and I get the LinkedIn messages as well. There are other ways that information is being pushed out, but I think the problem—the challenge is that that messaging is blunted by the fact that we still have no answers for many of the critical questions.

So rather than focusing on creating more forums for disseminating information, I think we need to focus on providing real hard information about how much this is going to cost and when are small businesses going to need it, what level are they going to need? Until we can answer those basic questions, I think, you know, the forums are going to be largely lost on the small business community.

Ms. VAN DUYNE. Thank you very much, Mr. Williams.

Mr. Dunbar, did you have anything to add?

Mr. DUNBAR. Yes. One of the items with small business is a lot of small businesses work from, I will say remote locations. You may have an office where you have people working from home, several people at various homes. One of the big items that was brought up

recently by one of the board members for the CMMC was that we will be subject to home inspections in order to pass CMMC.

So now you have people doing home inspections in your own private homes. The risks beyond that on there are just, you know, incalculable.

Another item to me that really piqued my interest there was our ability to protect ourselves during an assessment. Right now, an answer on the Board FAQ site basically states that an RP that helped us go ahead and put together our plan is not to be there to defend our plan. So if we get—you know, fail it, we are supposed to know this book again. We don't have an expert to know it.

Ms. VAN DUYNE. Excellent. Thank you very much.

I yield back.

Chairman PHILLIPS. The gentlelady yields back.

And now I recognize the gentleman from Pennsylvania, Mr. Evans, for 5 minutes.

Mr. EVANS. Thank you, Mr. Chairman.

Mr. Dunbar, what would you—what would be your recommendations for those businesses that are just learning about the Initiative? I would like to ask all of the panel that question.

I will start off with you, Mr. Dunbar.

Mr. DUNBAR. I honestly don't know that I have an answer for that, because trying to know find the information, it has not been clear enough to everybody where to get it. If I am getting it from LinkedIn, I mean, I first heard about it at an Army Corps Small Business Conference in 2019. Otherwise, I may not even know about it today.

Mr. EVANS. Does any other panel—any comments or thoughts on that, any of the other panelists?

Mr. SINGER. Sure, sir, I would like to make a comment.

You know, I think one of the important things is for companies to find reputable businesses to help support them through this process, and, unfortunately, I think there is too much variation in the help that they are getting, as Ms. Wilson spoke of earlier also.

I think also that, especially now, I think a lot of the level three companies are aware of this coming down, especially small manufacturers that are, you know, just now starting to really understand this because the letters are coming out from the primes.

But I think a big gap is the people that are going to have to meet level one and they don't know it right now, and I think that should be a much more proactive reach-out to those folks. I mean, the DOD knows who they are contracting with in these areas, and I think they should take a more active role.

Mr. WILLIAMS. Yes, Representative Evans, if I could just back up Mr. Singer's comments there, our primary recommendation to our small business clients is to get level one ready. The level one requirements really are basic things, like antivirus software and spam filters that we think all companies should be doing, regardless of whether you work with the Federal Government. In this day and age, you should be doing at least those basic requirements, and they are already in the FAR. The FAR requires these basic safeguards. That has been the requirement for a long time.

So, this really, frankly, shouldn't be surprising, but I totally recognize that it is, because small businesses have so much to focus

on. But these requirements are not new, and they are, generally speaking, not difficult to obtain for small businesses. So, we would like everyone to really focus on at least getting level one ready, because these are things you should be doing as a business.

Ms. WILSON. And I would echo everyone's comment that has been made on the panel. I do make a concerted effort to share with small business owners to mention CMMC, and I mention it in the context of the necessary need for them to actually have it, but understand what it means and the implications, because right now, we just have black and white implications of saying if you don't have it, and your contract comes up for renewal, then you run the risk of losing your contract.

And, so, putting that fear in them early on, maybe prompt them to move forward. But also I think from our perspective at T47, we have already proactively tried to secure something similar, certification. It may not be directly related, but to at least get us ready so that way when it comes down for us to have an audit, we are in a position to actually, pass the audit.

So it is a challenge, and right now, because we don't have cohesiveness of information, it makes it a little more difficult for small businesses that just now are recognizing that they need it, or they know they need it but don't know how to secure it.

Mr. EVANS. I yield back, Mr. Chairman.

Chairman PHILLIPS. The gentleman yields back.

And now I recognize the gentleman from Wisconsin, Mr. Fitzgerald, for 5 minutes.

Mr. FITZGERALD. Thank you, Mr. Chair.

I am going to start, Mr. Singer, as a fellow Wisconsinite, I have quite a bit of experience in working with obviously anywhere from major corporations down to, you know, one and two person Ma & Pa shops. But my question, I was talking a little bit to staff about this yesterday. We were kind of kicking around the idea that there might be a different level of security from State to State throughout the Nation, and I just wanted to get maybe your perceptions on, is there much interaction with the State of Wisconsin from your perspective? And if there are, what are the influences there? Because I think it would be valuable for Members of Congress to know kind of what is going on at the State level.

Mr. SINGER. Thank you, sir.

As a fellow Wisconsinite, it has been kind of fun starting a business in Wisconsin, and Minnesota too. But as far as—I haven't had a lot of interaction with the State government. I counseled them a little bit on CMMC. It has been new to them, in helping them to try and understand the issues around this for small business.

One of the organizations that we work very closely with are the MEPs, the Manufacturing Extension Partnership programs. Every State has one. There is—and Puerto Rico has one. We have been working very closely with them to try and help get the small manufacturers in Wisconsin and Minnesota through the assessment so that they can accept awards from the primes.

So I think that is really actually a good avenue to help small businesses is through the MEPs, especially the manufacturers. But I don't know that, you know, the States yet have really kind of fig-

ured out any good mechanisms to help fund or support the small businesses as of yet.

Mr. FITZGERALD. Very good. Thank you.

As anybody could probably answer this question, let me just direct it to Mr. Dunbar, though. And I apologize if some version of this was asked earlier. But cybersecurity, obviously, you can be a consultant, quote/unquote "consultant," and I am wondering if you are seeing, because we are starting to hear that there are many different versions of this, and obviously many different levels of professionalism and knowledge.

And I am just wondering if you could comment kind of, you know what is your take, kind of what is going on out there on the street?

Mr. DUNBAR. Thank you, sir.

Yes, you are 100 percent correct. There is a large fear in the small business community that the "consultants," in quotations, are not all equal. I get inundated with emails daily from companies trying to convince me that I am not ready, I need to be—I am losing my contracts. I mean, blatant lies in your inbox constantly from companies. I call it the fear marketing.

I have also seen things from—as one of the other members of the committee had mentioned earlier, you know, companies that—there are fraudulent companies out there, just that have no business. There was one, I think, the College of India was creating, We can get you CMMC certified.

Mr. FITZGERALD. Right.

Mr. DUNBAR. Like, okay, great. How is the College of India getting me CMMC certified? And that is a fear. We don't know where to go. We have been told, Oh, well, the only great place, the only authorized place is the CMMC-AB, if they are on their marketplace, that is the only place to get, that is legal, to get your consulting from. That is a whole separate issue, I believe.

Mr. FITZGERALD. Yes. And, you know, to dovetail on that, so compliance, too, because it is kind of wide open as to what the cost could be associated with that. You know, you hear figures thrown around, like, Well, it costs a company $10,000 to comply, or it costs them $1 million to comply. That is not necessarily a good gauge, I don't think, on, kind of, you know, whether or not somebody is a legitimate consultant. But it sounds like that is kind of the range that is out there when a lot of these small businesses are considering how to become not only compliant, but protect ourselves, so——

Mr. DUNBAR. And I think you raise a good point because there is also a lot of companies out there trying to sell one-stop shopping, like, Oh, we have this program. You buy this program, you are CMMC-compliant.

Mr. FITZGERALD. Right.

Mr. DUNBAR. And that is not going to happen.

Mr. FITZGERALD. Yes. Very good. Thank you very much.

I yield back.

Chairman PHILLIPS. The gentleman yields back, and that completes our questioning.

So I will move to my closing statement. And I want to thank all of our witnesses for a very compelling testimony today and for illu-

minating the very issues that small contracting firms are experiencing as they try to bolster their cybersecurity.

Recent high-profile attacks have made it very clear that the threat of malicious cyber actors is growing, and that is why we must ensure that companies in the DIB are prepared for all cyber threats that might come their way. But it is equally vital, equally vital that we do not deprive businesses like yours of critical opportunities in that process.

We have got to work as a committee to increase cybersecurity preparedness across the DIB in a way that is not cost prohibitive to small firms. By achieving this, the small businesses will still have ample access to a lucrative marketplace while also protecting themselves against 21st century threats.

I would ask unanimous consent that members have 5 legislative days to submit statements and supporting materials for the record.

Without objection, so ordered.

And if there is no further business to come before the committee, we are now adjourned.

Thank you.

[Whereupon, at 11:17 a.m., the subcommittee was adjourned.]

APPENDIX

Testimony of Jonathan T. Williams
Partner, PilieroMazza PLLC

Hearing entitled:
"CMMC Implementation: What It Means for Small Businesses"

Subcommittee on Oversight, Investigations, and Regulations
Subcommittee Hybrid Hearing

June 24, 2021

Chairman Phillips and distinguished Members of the Subcommittee, I would like to express my sincere thanks for the invitation to submit testimony for this hearing of the Subcommittee on Oversight, Investigations, and Regulations. I am honored to present my perspective on the Department of Defense's ("DOD") Cybersecurity Maturity Model Certification ("CMMC") initiative, how it is intended to work, the current status, and the questions and concerns that many small business contractors have regarding CMMC.

My name is Jonathan Williams. I am a partner with PilieroMazza PLLC, a law firm based in Washington, DC. I have practiced law for 20 years and nearly all this time I have spent working with government contractors, with a focus on small businesses. Many of our clients at PilieroMazza are small and mid-sized government contractors that work with DOD agencies as both prime contractors and subcontractors. I am also a member of the Board of Directors for the HUBZone Council, a member of the Montgomery County Chamber of Commerce's GovConNet Council, and our firm serves as General Counsel for the National Veteran Small Business Coalition ("NVSBC"). In these capacities, we have frequently communicated with small business contractors and their representatives regarding the CMMC initiative, which has been a very popular and divisive topic amongst the small business community since it was announced a few years ago.

I am testifying on behalf of myself as well as on behalf of my colleagues at PilieroMazza. My testimony is based on our understanding of the CMMC initiative and our experiences in representing small businesses that work with the federal government.

Overview of the CMMC Initiative

DOD's emphasis on cybersecurity has been steadily growing for many years. In November 2013, DOD first implemented the contract clause at DFARS 252.204-7012 and required defense contractors to comply with certain controls in the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53. Over the years, DOD revised the "7012 clause" to cover controlled unclassified information ("CUI") and require defense contractors handling such information to comply with the 100+ security controls in NIST SP 800-171. More recently, with its "Deliver Uncompromised" strategy and elevation of cybersecurity to the "Fourth Pillar" of DOD acquisition planning (along with cost, schedule, and performance), DOD has left no doubt about the importance it has placed on enhancing cybersecurity for the defense industrial base ("DIB").

DOD's focus on strengthening the cybersecurity of the DIB is well-founded and necessary. As our businesses and our lives are increasingly conducted in and dependent upon cyberspace, we are that much more vulnerable to all manner of cyberattacks and loss of sensitive information. Recent news stories like the pipeline shutdown and resulting gas shortages put the importance of cybersecurity in stark relief.

To this point, DOD's cybersecurity measures for contractors such as the "7012 clause" have relied on the contractors to self-certify to their compliance. DOD does not have adequate time or resources to audit but a relatively small portion of the vast DIB. As a result, the critical cybersecurity measures put in place to protect our Nation's sensitive defense information have largely depended on an honor system.

Against this backdrop, DOD is moving to CMMC. First announced in 2019, CMMC marks a significant change in DOD's approach to cybersecurity for the DIB because the CMMC initiative will end self-certification. Rather than relying on the contractors to assess themselves, CMMC will require contractors to undergo a review by a third party that will assess the contractor's "cybersecurity hygiene" against various cybersecurity benchmarks. And, to ensure adequate protection across the entire DIB, DOD will require that all DOD contractors (both prime contractors and subcontractors) – regardless of the nature of the work the contractor performs – must have CMMC. The only exception is for contractors that solely provide commercially available off-the-shelf ("COTS") items; otherwise, every contractor that does business with DOD must obtain CMMC.

The applicable benchmarks to obtain CMMC were first set forth in version 1.0 of the CMMC controls, which were released on January 31, 2020. CMMC has five levels, with Level 1 being the lowest, Level 5 being the highest, and Level 3 being the minimum requirement to process CUI. All levels are cumulative, so a Level 3-certified contractor must perform all of the Level 1 and 2 requirements in addition to the Level 3 requirements. The levels come with both "practice" and "process" requirements, where "practice" is day-to-day compliance with applicable controls, and "process" is the extent to which those controls are embedded in the contractor's organization. DOD visualizes the levels in the following manner:

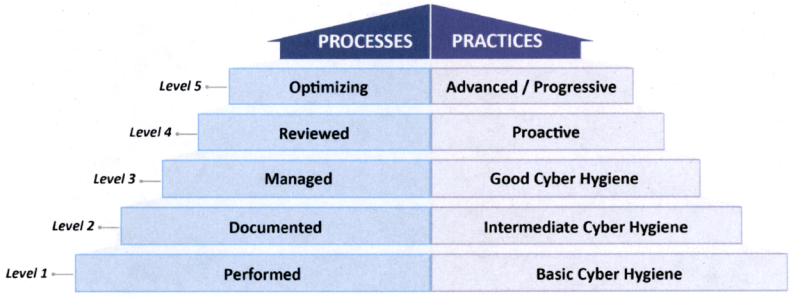


Figure 2. CMMC Levels and Descriptions

For Level 1, contractors must comply with the basic cybersecurity safeguards outlined in FAR 52.204-21, which already exists and applies to most contracts. The basic cybersecurity safeguards required under FAR 52.204-21 and CMMC Level 1 include using a spam filter for emails, installing and enabling antivirus software, requiring usernames and passwords to log on to company systems, and escorting visitors to prevent unauthorized system access. Level 1 is intended to be attainable for small businesses, at a relatively low cost. A Level 1-certified contractor may only handle federal contract information ("FCI"), which is a broad term for any information that relates to federal contracts. However, CMMC Level 1 is not high enough for handling CUI. A contractor that handles CUI must have at least CMMC Level 3.

Level 2 is a transitional level between 1 and 3, and generally is not a level at which contractors will specifically aim. Indeed, it is unlikely that DOD will issue contracts that require Level 2 thus making this a largely superfluous level. In my view, small business contractors will decide between Level 1 (if they only handle FCI) or Level 3 and above (if they handle CUI).

Level 3 allows contractors to handle CUI and is expected to be the requirement for many DOD contracts. Level 3 incorporates all the NIST SP 800-171 rev. 1 security controls, as well as a few CMMC-specific controls. Level 3 requires contractors to, for instance, use FIPS-validated encryption modules to store sensitive information, block company computers from accessing known malicious websites, review code associated with internally-created applications for mistakes and vulnerabilities, and keep abreast of cyber threat intelligence information and update threat profiles, vulnerability scans, and risk assessments. The contractor's policies and procedures for complying with the various security controls necessary for Level 3 must be documented in a system security plan ("SSP") and actively managed by the company.

Levels 4 and 5 concern "advanced" cybersecurity hygiene and are intended to be applied when there is a high likelihood of "advanced persistent threats." DOD accordingly estimates that these levels will not be applicable to the vast majority of contractors in the DIB.

To obtain CMMC, contractors will need to contact third-party certifying organizations, referred to as C3PAOs. Contractors will apply for a particular Level and the C3PAO will evaluate the contractor's systems to determine whether they meet the requirements for that Level. C3PAOs may certify a contractor only up to the requested Level, so if a contractor requests a Level 3 certification, the C3PAO may certify the contractor at Levels 1, 2, or 3, depending on which requirements the contractor meets, but not at Levels 4 or 5. The certification is expected to be valid for three years. How much it will cost and how long it will take for contractors to go through the certification process with the C3PAO are still unknown.

DOD has indicated it intends to roll out CMMC using a "crawl-walk-run" approach. In late 2019 and early 2020, DOD estimated that it would require CMMC certification in 15 "pathfinder" contracts by the end of FY 2020, and that all DOD contracts would require CMMC certification by the end of FY 2025. However, shortly thereafter, the COVID-19 pandemic struck, and the timeline has been delayed. Currently, DOD indicates at least seven and up to 15 contracts will require CMMC in FY 2021. The number of CMMC-covered contracts is

forecasted to increase to approximately 75 in FY 2022, with the ultimate goal of requiring all DOD contractors to have CMMC by FY 2026.

Part of the reason for the delayed implementation of CMMC is the lack of C3PAOs. The CMMC Accreditation Body ("CMMC-AB") was established in early 2020 to handle the accreditation of C3PAOs. As of June 21, 2021, the CMMC-AB has approved two C3PAOs, and it appears both were approved very recently.

CMMC will be incorporated into individual DOD contracts via a pending DFARS clause. This means that the CMMC Level required for a particular contractor will depend on the CMMC Level(s) incorporated into the contracts on which that contractor works. Accordingly, it is difficult for small businesses to predict when they will need CMMC, or what Level(s) they will need. For most small businesses, they understand CMMC may be a requirement for them at some point between now and FY 2026, but beyond that is largely unknown.

When DOD begins including CMMC in solicitations for new contracts, it will be required by the time of award rather than at proposal submission. It remains unclear how DOD will handle potential bottlenecks in the certification process, which may prevent timely approval of CMMC. With only the two approved C3PAOs so far, there is a potential for significant backlog in the application process. Application delays may put the award of DOD contracts behind schedule or it may jeopardize certain contractors' abilities to receive new contract awards if they are unable to receive timely approval of their application for CMMC.

Further, DOD has not yet released the final rule that will allow contracting activities to place CMMC requirements in contracts, and provide specific guidance related thereto. While DOD has released a proposed rule, DOD has stated that there may be significant differences between the proposed and final versions of the regulations. It is obviously important for contractors to have the benefit of the final rule to solidify and understand the requirements.

When DOD issued the proposed rule on CMMC last year, it also implemented an "enhanced" self-certification system. This interim measure requires contractors that process CUI to complete a self-assessment and self-scoring based on the NIST SP 800-171 controls, which the contractor uploads, along with their SSP, to the Supplier Performance Risk System ("SPRS"). Most contractors need only submit the self-assessment and score to SPRS, and DOD will audit only a small percentage of those assessments and scores. The new self-scoring requirement is modified self-certification, insofar as it includes evidence that the contractor performed a self-assessment and the results. It is not yet clear how or if DOD intends to use the SPRS self-assessments in the CMMC certification process. DOD has stated that this issue, as well as the other issues noted herein, will be examined in the final rule.

As far as most small business contractors are concerned, there has been little practical impact from CMMC to date. While I know of several small business contractors that have proactively sought to get ahead of the coming CMMC requirements and have made the necessary investments to be ready for CMMC, the vast majority of small businesses with which we work are still taking a "wait and see" approach. In particular, they are waiting to see when CMMC will be required for their business, how the certification process will work, and how much it will

cost. Coupled with the slower-than-anticipated rollout of the C3PAOs and the CMMC DFARS clause, there is a significant potential that many small business contractors will be caught off guard with insufficient time to prepare, apply, and obtain CMMC in time for when it is needed for their contracts. That is not to say that there has been insufficient warning to the small business community about CMMC; there has been a significant push by DOD and others since 2019 to get the word out. However, in my experience, that impact of that messaging has been blunted by the realities of running a small business, more existential business concerns caused by COVID-19, the elongated rollout of CMMC, and the many questions that remain unanswered such as when small businesses will need CMMC, how the certification process will work, and how much it will cost.

Suggestions to Assist Small Businesses

From my experiences discussing CMMC with small businesses, one of the biggest areas of concern is that there remain more questions than answers on key aspects of the initiative. In particular, small businesses are concerned about how much CMMC will cost (both to obtain the certification and to implement the internal steps necessary to maintain the certification), what CMMC level DOD agencies and prime contractors will require of small businesses, and how much time it will take to obtain the certification. I have the following suggestions that I believe would make CMMC easier to digest for small businesses.

- **Enhance the Small Business Administration's ("SBA") All Small Mentor-Protégé Program ("ASMPP").** The ASMPP is a critical tool for small businesses to obtain necessary resources and other assistance from their mentors, and we have seen first-hand the many success stories this program has helped to write for small businesses. The ASMPP could be enhanced to explicitly provide that mentors are expected (or at least encouraged) to assist their small business proteges in obtaining CMMC, including by providing financial and technical resources needed for the certification. The same could be done through DOD's mentor-protégé program. Mentors should be encouraged to use these relationships, which provide many benefits to mentors, to help ensure the protégé firms are not left behind as the CMMC initiative continues.

  Additionally, SBA should remove the current limitation that small businesses may only ever have two mentors. Allowing small businesses to have more mentors would increase the ability of small businesses to use the ASMPP to obtain procurement, technical, and also CMMC assistance from multiple mentors that may be able to provide mentoring in some but not all of these different areas.

- **Do Not Require CMMC for Unpopulated Joint Ventures ("JVs").** Together with the ASMPP, many small businesses utilize JVs in pursuing set-aside contracts. These JVs are "unpopulated," meaning they do not have their own employees, business systems, and other certifications. Instead, the JVs rely on the employees, systems, certifications, etc. of the JV partners. Yet, based on the FAQs on the CMMC-AB website, it appears a small business JV will be required to obtain CMMC. Requiring the small business JV to obtain its own CMMC does not make sense because the JV will not have its own IT system or employees. Such a requirement would add unnecessary time and expense for

small business joint ventures, unfairly diminishing their ability to compete for federal contracts. The requirement for the JV itself to have CMMC is also contrary to the following regulation that SBA recently implemented stating that:

"When evaluating the capabilities, past performance, experience, business systems and certifications of an entity submitting an offer for a contract set aside or reserved for small business as a joint venture established pursuant to this section, a procuring activity must consider work done and qualifications held individually by each partner to the joint venture as well as any work done by the joint venture itself previously. A procuring activity may not require the protégé firm to individually meet the same evaluation or responsibility criteria as that required of other offerors generally. The partners to the joint venture in the aggregate must demonstrate the past performance, experience, business systems and certifications necessary to perform the contract."

13 C.F.R. § 125.8(e) (emphasis added). Consistent with this SBA regulation, CMMC should not be required from small business JVs. Instead, a small business JV should satisfy the requirement for CMMC on a given DOD contract as long as at least one of the JV partners that will handle the covered information on the contract has the necessary level of CMMC.

- **Provide for Expedited Review of Pending CMMC Applications if a Small Business is Selected for Award.** CMMC will be required by the time of award, rather than at the time of proposal submission. While this is beneficial because it permits small businesses to submit proposals for prime contracts and subcontracts before obtaining the necessary level of CMMC, there may not be enough time between proposal submission and award for the small business to complete the certification process (the timelines for which are still unknown). It is also unclear how soon small businesses will be able to apply for CMMC or if they will be able to apply before they have a need based on a pending solicitation. Moreover, some large business prime contractors may not be willing to enter into teaming or subcontract agreements with small businesses if it is unclear when the small business will obtain its CMMC. To address these concerns, I suggest an approach similar to how SBA is currently handling its new woman-owned small business ("WOSB") certification program. In particular, small businesses should be allowed to submit a proposal for a prime contract or subcontract that requires CMMC as long as the small business' CMMC application is pending with a C3PAO at the time of proposal submission. And, if the small business is later selected for award of the prime contract or subcontract, this should require the C3PAO to "fast track" the small business's application if it is still pending.

- **Build in Flow-Down Protections.** Many small businesses are concerned that, despite DOD's statements that the majority of small businesses will only need CMMC Level 1, the reality will be that many more small businesses will have to obtain CMMC Level 3 or above based on the requirements imposed on them by prime contractors. Given there is often a significant imbalance in the negotiating positions of large prime contractors and small business subcontractors, it is not enough to leave it to the prime contractors and subcontractors to negotiate over the appropriate level of CMMC for subcontracts. The

DFARS should be protective of small business subcontractors in this regard by prohibiting prime contractors from flowing down a higher level of CMMC than is necessary based on the subcontractor's scope of work. I understand the prime contractor's perspective and the risk they face in flowing down lower levels of CMMC to their subcontractors. However, to the extent we must balance risks, we should err on the side of encouraging small business participation and not creating an artificially high barrier by allowing prime contractors to reflexively require a higher CMMC Level from their subcontractors beyond what is necessary based on the scope of each subcontractor's work. The onus should be on prime contractors to manage their subcontractors' roles and how they access information from the prime contractor and to be judicious in determining the appropriate CMMC Level for each subcontract.

Additionally, because of the negotiating imbalance that typically exists between larger prime contractors and small business subcontractors, subcontractors should be permitted to contact the contracting officer directly to seek confirmation of the appropriate level of CMMC for the subcontract, in the event of a disagreement between the prime contractor and subcontractor.

- **Encourage Flexible Approaches Such as Secure Enclaves.** For small businesses that need to access CUI in the performance of their prime contract or subcontract, there should be flexibility to utilize arrangements that would not require the small business to have that information in its IT system. If the small business is required to obtain CMMC Level 3, there will very likely be a significant cost difference compared to Level 1, and this Level 1 vs. Level 3 determination will likely be a significant barrier to entry for small businesses that cannot afford the sizable investment to jump from Level 1 to Level 3.

  A good example of the challenges many small businesses will face with CMMC comes from the construction industry. The majority of small businesses that have reached out to me for help understanding and preparing for CMMC have been construction firms. Unlike their counterparts in more IT-focused industries, small business construction firms on average are less likely to have the in-house capabilities to prepare for CMMC Level 3. Yet, these firms may be subjected to CMMC Level 3, requiring a significant investment in external resources, if the construction plans and specifications with which they work enter their IT system and are labeled as CUI. The cost and technological challenges to obtain CMMC Level 3 will be prohibitive for many small businesses like the construction firms with which I have spoken.

  That is why I hope we can develop flexible approaches that would allow more small businesses to qualify at CMMC Level 1 and avoid the additional investment needed for Level 3. For some small businesses, there will be no avoiding Level 3 and that will be a necessary investment for them to make. But for others, like small construction firms that may only handle a few discrete plans or specifications labeled as CUI, it would be ideal to develop a workaround that would permit them to still work on the project but at CMMC Level 1. These firms could potentially avoid CMMC Level 3 if the DOD and/or the prime contractor maintains the CUI in its own IT system, and then gives the small business access to the information on the DOD or prime contractor's IT system in a way

that would promote the security of the information but would also permit the small business to qualify at CMMC Level 1 rather than Level 3.

- **Consider a Cybersecurity Grant for Small Businesses.** Many small businesses are concerned about the cost of obtaining CMMC, both the cost of the certification process and also the internal costs that will be needed to come into compliance and maintain the certification. While the government may ultimately bear these costs through increased pricing from contractors, for many small businesses, it will be difficult if not impossible to find the resources to make this upfront investment. To help address our critical cybersecurity infrastructure across the small business DIB, Congress could consider establishing a small business grant program and/or a low or no interest loan program that would facilitate small businesses in making the necessary investments to strengthen their cybersecurity hygiene and obtain the necessary level of CMMC.

In closing, the CMMC initiative appropriately aims to improve our Nation's cybersecurity posture and better protect our sensitive information. I do not think small businesses would debate the importance of cybersecurity, or that doing business with the federal government is a privilege, not a right, which requires investments in compliance and infrastructure. At the same time, the worthy goals of the CMMC initiative must be calibrated to avoid creating an unnecessarily high barrier to entry for small businesses, which are the engine of our economy and critical partners with the federal government for innovation and provision of many necessary services and supplies. Small businesses need sufficient understanding of and time to plan for CMMC, resources, and judicious application of the new requirements that promotes, rather than prevents, small businesses from continuing to play a vital role in the DIB as prime contractors and subcontractors.

Thank you again for the opportunity to submit this testimony.

Statement of Scott Singer

President, CyberNINES

before the

House Committee on Small Business

Subcommittee on Investigations, Oversight, and Regulations

Hearing on "CMMC: What It Means for Small Business"

June 24, 2021

316 W Washington Ave. STE 600
Madison, WI 53703

CyberNINES llc | CyberNINES.com |
(608) 512-1010

With offices in Minnesota, California and Wisconsin

Statement of Scott Singer
President of CyberNINES

Thank you Representative Phillips, Ranking Member Representative Van Duyne and members of the subcommittee for inviting me to testify this morning. I look forward to providing information that will help ensure we have a secure Defense Industrial Base and find cost effective solutions to allow small businesses to fully comply with the CMMC Framework and the Department of Defense Federal Acquisition Regulation Supplements.

The SolarWinds hack, Colonial Pipeline cyberattack and the JBS cyberattack have all been in the news lately. There has been some discussion on whether or not implementing NIST SP 800-171 and/or the CMMC practices would have prevented the attack, but in my opinion, it could have prevented having to pay the ransoms and the lost data would have been encrypted and of no use to the perpetrators.

While I will discuss some areas where we will need to relax some requirements, this is done with the suggestion of using a risk-based approach. The faster we can make progress towards getting the DOD supply chain secured the safer it will be.

My name is Scott Singer and I am an owner and President of CyberNINES, a Service-Disabled Veteran-Owned Small Business. CyberNINES has embraced the CMMC ecosystem and is both a Registered Provider Organization (RPO) and a candidate for becoming a Certified Third-Party Assessor Organization (C3PAO).

I am also a retired Navy CAPT and spent over 30 years in active and reserve rolls. My last active-duty role was at the FEMA NRCC (National Response Coordination Center) as the DOD Liaison at the end of 2017, post Hurricanes Irma and Maria. I have over 26 years of experience in information technology leadership roles at Fortune 500 companies and smaller. I tell you this to give the committee some background on myself and the fact that I have worked in both large and small organizations.

CyberNINES formed in June of 2020, an interesting time to start a new business. Thanks to the Interim Final Rule released on Nov 30, 2020, we have been busy. Small businesses are now getting the word they need to comply with NIST SP 800-171. This has come about through the requirement for all DOD contractors in the supply chain to post a cybersecurity compliance score in the Supplier Performance Risk System (SPRS). This requirement is the same no matter

whether you are a Prime Contractor or a sub of a sub of a sub. Primes are responsible for ensuring their supply chain is compliant and I have been seeing more of that happen as of late.

CyberNINES has partnered with MEPs (Manufacturing Extension Partnership) in Minnesota (Enterprise Minnesota) and Wisconsin (WMEP). MEPs are public-private partnerships located in all 50 states and Puerto Rico. They focus on supporting small and medium-sized manufacturers. MEPs are an initiative of NIST, a major component of the Department of Commerce.

I suspect I have done assessments in the districts of a number of the members of this subcommittee.

COMPLIANCE COMPLEXITY

Small businesses do not have purchasing departments. They do not have compliance or regulatory departments. In most cases they have not gone to any classes on government contracting and barely know what a flow-down (requirements passed down to subcontractors on purchase orders) is let alone how to protect ITAR (International Traffic in Arms Regulations), EAR 600 Series (Commerce controlled items that used to be controlled as ITAR) or CUI (Controlled Unclassified Information). Those of us that work with NIST SP 800-171 and CMMC all day may start feeling like we know it but for those that don't it is a daunting set of Acquisition Regulations, Export Control Regulations and cybersecurity contract clauses. I have seen Primes flow-down pages of requirements to a small business along with pointing them to their website for more. We need to make this process easier for them. Primes, C3PAOs and RPOs can assist these small businesses get compliant and reduce the complexity for them. **However, the small businesses need help funding this journey or they will drop out of the Defense Industrial Base.**

COSTS ASSOCIATED WITH MEETING CMMC AND MAINTAINING COMPLIANCE

Cybersecurity compliance scores required to be posted in SPRS range from a low of -203 to a perfect score of +110. Of the last 33 Basic Assessments we have conducted for small businesses, the average compliance score was -105. The median score was -110 (where most companies fell). The low was -197 and the high was -13. I would like to think of us as experts and we are only at +81. My business needs to be fully compliant at +110 and complete 20 more CMMC Practices before we are able to be assessed by DCMA DIBCAC (Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center) and get authorized by the CMMC Accreditation Body to conduct assessments for the DOD. So, for our 33 small businesses in WI and MN, where we have recently conducted a Basic Assessment, we

have found that on average they are only about 34% of the way toward meeting all the NIST Controls. Cost models put forth by the government assume that companies are much further along on this journey and have completed the 110 NIST Controls and only have to complete the 20 new CMMC Practices, get assessed by a C3PAO and they will be compliant. Assuming fully compliant to the 110 NIST Controls, the DOD has put out that this will cost an additional $26,214 to complete the 20 Practices and 3 Processes followed by an additional $28,616.24 to be assessed by a C3PAO. Reality paints a different picture. As discussed above small businesses that we have assessed are only part way there and the costs will be much higher. Our estimates indicate that they will be more to the tune of $130,000 from my cost models (for micro companies).

Last week I conducted a Basic Assessment of a small manufacturer in MN. They had only 6 employees (including the owner and his wife), one small manufacturing space with three machines and they do excellent, innovative work. I spent a good majority of my time doing the assessment from the owner's house. This year he expects to make $875,000 in revenue. My estimate is that if he wants to stay a DOD contractor and meet CMMC by 01 OCT 2025, he will have to spend 10% of his revenue over the next three years alone on getting compliant. Obviously, his company will not be able to absorb this and we could lose a highly innovative parts supplier to the DOD.

Small businesses lack expertise in regulatory, DOD contracting, quality systems and information technology requiring an excessive amount of opportunity costs for a small business that tries to forge their own path to compliance. There are tools that can help small businesses comply but we need to help connect them with resources that will guide them toward cost effective solutions instead of selling them expensive tools. **Having a program where the Primes take a strong guiding hand of their supply chain is critical to maintaining these small businesses as DOD suppliers.**

There are a lot of discussions around the costs associated with being CMMC compliant as an allowable expense. To the best of my knowledge, Maturity Level 5 (ML5) contracts will be able to direct charge their allowable cybersecurity expenses. For ML3 and Maturity Level 1 (ML1) (which will be the requirement for the vast majority of the DIB) they are directed to add the costs to their indirect rates and spread the costs across the business. I contend for the small manufacturers that this only works if they are the Prime. Most don't have established indirect rates and most don't do cost-reimbursement contracting for DoD. Moreover, market factors around competition for orders will require them to compete and lower prices. Established contractors will be more likely to be able to provide a lower bid and win the order from the Prime. **There should be a process separate from the competitive market place to allow small**

businesses to get paid for the reasonable, necessary and allowable cyber compliance expenses. Companies further ahead should not be penalized and be able to recoup their past expenses too.

OPERATIONAL TECHNOLOGY REALITIES

One of the basic premises of both NIST SP 800-171 and CMMC is that CUI should be encrypted. In the last 33 assessments CyberNINES has done, none of the CNC (Computerized Numerically Controlled) machines being used by our clients would be able to support this requirement. NIST SP 800-171 does have some leeway for what is called Enduring Exceptions using compensating controls as outlined in the NIST SP 800-171 Assessment Methodology. CNC machines are used for generating parts through a reductive process from stock material in an automated fashion from a parts program. The vast majority of CNC machines do not allow for encrypted parts programs. The parts programs must be entered in the machine unencrypted and normally via a USB thumb drive.

To date and to the best of my knowledge, there are no pieces of CNC equipment utilizing encryption. And there are no plans of adding this option to CNC equipment that I am aware off.

CNC's are being used as an example here today, but most of the manufacturing machinery in industry faces the same challenge. Currently there are limited options for equipment that utilizes encryption. Those products utilizing encryption are very new to the market and not in mass use.

CMMC doesn't really address operational technology such as manufacturing equipment. I would propose that the CMMC standard expressly allow for compensating controls. We have been counseling our clients to protect the USB drives by locking them away when not in use, labeling the drives as CUI and protecting the parts program using a FIPS 140-2 compliant encrypted location such as a FedRAMP High GovCloud. And, our first choice is to air gap the equipment, but, when it needs to be connected to the Internet or Intranet, we recommend a defense in depth strategy of segmenting these manufacturing machines from the rest of the network. This can take time and cost money so some flexibility in implementation is essential.

BOTTLENECKS FOR C3PAOS

C3PAOS NEED TO GET ASSESSED SO THEY CAN DO ASSESSMENTS

As of the writing of this testimony only two companies have passed the DIBCAC assessment to be Authorized C3PAOs to conduct assessments. To the best of my knowledge, less than 10 C3PAOs will have been assessed by DIBCAC this year. According to the April 2021, CMMC Town

Hall, the Accreditation Body (AB) has recognized 171 Candidate C3PAOs and 278 pending C3PAOs: more than 400 total. In addition, there needs to be enough CMMC Assessors (CCAs) to conduct the number of assessments which the AB requires of C3PAOs. At this time there are only 100 Provisional Assessors (PAs) available to do assessments for C3PAOs. Doing the math, I don't see how we can get anywhere near enough C3PAOs through the process to assess 300,000 DIB companies by 01 OCT 2025. I saw one estimate that we would need over 8,000 assessment team members working full time from today until 01 OCT 2025.

C3PAOs must meet FedRAMP High in order to pass DIBCAC assessments. Requiring FedRAMP Moderate as is the current requirement for NIST 7010 would improve throughput of C3PAO assessments.

C3PAOs may only be holding System Security Plans (SSP) from consulting arrangements, and there is an argument to be made that they don't need to have client documentation in their environments related to assessments (Note: A C3PAO can't do an ML1 or ML3 Assessment and provide consulting to the same company). It is more likely the general consultants like RPOs will hold documentation such as System Security Plans and Plans of Actions and Milestones as they prepare organizations to be compliant. Thus, there is more risk, I contend, with RPOs than C3PAOs as C3PAOs should leave their work at the client's office. I believe a more appropriate level for C3PAOs is Maturity Level 1 (ML1) which is required for handling Federal Contract Information (FCI). However, in the interest of compromise, ML2, while a transition step, may be a good interim step to get more C3PAOs authorized if the DOD is set on ML3. That said, it has been helpful for my company to go through the same process as our customers. C3PAOs will be required to hold and submit assessment reports to eMASS. These assessment reports are being considered at this time as CUI which is also driving the ML3 requirement. A group of C3PAO candidate companies believe that this decision to treat these reports as CUI should be reviewed given the lack of CUI in these reports. (Over-classifying private information as CUI can create many problems disproportionate to value.) Doing so will permit a more appropriate and immediate number of C3PAOs to launch the CMMC program while still meeting the intent of handling CUI. **A compromise would be to assess Candidate C3PAOs to ML1 or ML2 now and require ML3 in the future, if needed, after more DIB companies get assessed. Recommend the DOD look at creating an eMASS Enclave to allow C3PAOs to use the tool without having to meet cleared industry requirements.**

C3PAOS STAFF MUST HAVE TIER 3 INVESTIGATION

C3PAOs have been instructed that the following staff need Tier 3 Background investigations. These investigations are equivalent to a DOD SECRET clearance investigation, but do not convey a clearance.

- All assessors

- Quality leads and technical managers responsible for assessment quality and review
- IT staff

This background check requirement is far above the standard for the assessment industry as well as the defense contractors being assessed. Even companies that develop ITAR products do not need Tier 3 background investigations of their staff.

The ability to submit staff for Tier 3 Background investigations is extremely limited at this time. C3PAOs have been advised to hire staff with active clearances as a workaround. This could negatively impact resources that could be used on cleared contracts.

This requirement for Tier 3 background investigations for assessment and support staff creates a bottleneck for C3PAOs. **I would recommend this requirement be reduced to the level of a typical government Suitability Determination. This would greatly increase the time to get people checked and I believe does not impact national security due to the level of information (CUI, ITAR, 600 Series) that is being reviewed. Another option is to allow interim clearance as done with DOD clearances.**

POSSIBLE SOLUTIONS

ALLOW RISK ACCEPTANCE

Right now, companies can't get a CMMC certification, when it is required, without a 100% score on all assessed criteria. Forcing a framework that requires such "perfect" compliance will result in DOD supply chain interruptions. In my experience with AS9100, ISO 13485 and ISO 9001, auditors are given some freedom to give major and minor findings. Failing only happened after multiple major findings and a failure of the company to address them. To my knowledge, the DOD has not been able to fully implement their own cybersecurity requirements for internal Federal Systems. 100% compliance is not a realistic goal.

I would suggest allowing companies to fall short on low risk cybersecurity requirements with provisional certification. In addition, I would recommend developing a scoring model for CMMC and a criterion for provisional certification, adjudicated by the DCMA DIBCAC. Rate suppliers as High, Moderate and Low and set a score for that level. As the process matures, the criteria for a pass should get harder. I think the idea of a provisional certification that allows companies to process CUI is best for balancing risk with the need to maintain the DIB supply chain in the short term.

ALLOW FOR REIMBURSEMENT OF SOME EXPENSES TO MEET CMMC

As discussed earlier in my testimony, non-COTS (Common off the Shelf) manufacturers are going to need to meet CMMC ML3, and small businesses are going to have a difficult time. While large Primes at CMMC ML5 are allowed to claim the allowable cybersecurity expense, ML3 and ML1 will need to absorb the cost in their indirect rate. Leaving it to market conditions for non-Primes will lead to an unfair playing field for competition. Those that want to take a risk or those that are further along with their own journey toward full compliance will be able to set lower prices and win orders. Those that decide to increase their internal indirect overhead costs and thus increase their direct rates will risk losing orders. While on the surface this may seem like fair competition, it is not in the best interest of the government in getting the best manufactured parts. There should be a system for reimbursement that is outside the competitive market process. For small manufacturers, use the MEP network as a way to equitably distribute funds. They are already setup to work in this fashion through NIST.

ALLOW HOSTING OF UNAFILLATED ORGANIZATIONS

There needs to be the allowance to support hosting of micro-small businesses on shared or higher lever suppliers in the supply chain without them needing to be ML3 Certified. As long as their host is certified. Using an MSSP (Managed Security Service Provider) model will allow sharing of costs of being compliant over a number of companies.

Another area of CMMC focus has been on using CUI Enclaves to wall of CUI from the rest of the company and reducing risk of a CUI breach. This is important for protecting CUI and can reduce costs for small businesses, but I believe there are some unintended consequences. Too much focus on CUI Enclaves could impact overall security. While encrypting CUI will ensure that it does not fall into bad actors, ransomware can take down the whole company and interrupt the DOD supply chain. Money may be better spent on general cybersecurity hygiene for small businesses and utilizing a hosting model from Primes. Create the hosting/ransomware protection framework for small to micro-DOD subcontractors.

GRADUATE THE ROLL OUT OF CMMC

Start the roll out based on risk. Develop a risk level for orders similar to Rated Orders. Require higher risk orders to have to meet the CMMC requirement along with the Prime's supply chain. The risk should be based on the impact to national security due to a breach of CUI or impact to a project due to ransomware. I would recommend this going into place at the same time that CMMC goes into effect on 01 OCT 2025. Before then, the CMMC process should be tested thoroughly. Gradually increase the number of required Primes and their supply chains that must meet the requirement based on the ability for the C3PAO and CMMC ecosystems ability to handle the demand.

Small businesses further down the supply chain generally are dealing with single parts and special processing (painting, coatings) whereas larger suppliers are dealing more with sub-assemblies. In addition to risk rating awards, I recommend that CUI at the part level should be viewed as less of a national security risk than assemblies (this will not always be the case).

CONCLUSION

The Defense Industrial Base is critical to our national security. The majority of the 300,000 contractors in the DIB are small businesses. Without monetary support and clear regulatory guidance, the DOD will lose small businesses as they will make the tough business decisions to find business in the commercial sector.

A balance must be struck between risk and cost. Too much cost and we lose suppliers. Too much risk and we hurt our National Security.

Thank you for allowing me to testify today. And, especially, thank you for supporting all the small businesses that are the backbone of our National Security.

T47 International, Inc. (T47) Testimony Prepared for
The Committee on Small Business
Members, Subcommittee on Oversight, Investigations and Regulations

Subject: CMMC Implementation: What it Means for Small Businesses
Presented by: Tina Wilson, Chief Executive Officer (CEO)

Chairman Dean Phillips, Ranking Member Beth Van Duyne, and Members of the Subcommittee, thank you for the invitation to testify today.
I am Tina Wilson, CEO – T47 International and I am honored to have the opportunity to speak to you and provide some insight regarding the implementation of the Department of Defense Cybersecurity Maturity Model Certification (CMMC) initiative.

This initiative is extremely important to protect our nation's Defense Industrial Base, supply chain, intelligence products and assets, and information technology infrastructure. As a Nation, we are at a critical juncture in our history, where cyber is our new warfare and the urgency to provide sustainable solutions to protect everything that IT touches is essential.

As a business owner with over 260+ employees, located in over 28 states and overseas, T47 provides a variety staffing services from budget and finance, janitorial, inventory management, aircraft tools maintenance, to mailroom and non-clinical medical and dental case managers. The diversity of service offered, puts me in a unique position to provide a different perspective regarding this subject and the implications. Most of our employees understand the meaning of cyber security but we have a handful that may not. Therefore, training them will be key to cyber defense.

As CMMC standards continue to be developed and incorporated into contracting agreements and modifications, it is essential that the small business committee be aware of the policy implications, if the CMMC standards are not clearly communicated and monitored for fraud, the financial ramifications to the over 300,000 defense industrial base of contractors, especially to the small business community could be devasting. Based on this statement, I will cover three main subject areas of concern and offer recommendations:

1. Cost to Secure CMMC
2. Cost Not to Secure CMMC
3. Audit Impostors

Cost to Secure CMMC
As of today, there is no set cost to obtain the CMMC. The CMMC Accreditation Body has stated that the marketplace will need to define the cost, which leaves it wide open for interpreting what this cost will be. Whether it is a tiered cost based on the size of the business or a set cost regardless of the size, there will be a initial and sustain cost that will impact a small business ability to secure the certification. Providing estimates of implementation costs, including and especially by tier, would allow companies to better predict future business expenses and plan for compliance. As of today, T47 is undergoing three International Organization for Standardization (ISO) and one of the ISO 27000 which is information technology – security for any kind of digital information. This certification is believed to be similar to what companies may expect for

a CMMC certification and is approximately $28,000 - $35,000 to obtain and takes approximately six (6) to eight (8) months to implement. This is a tremendous cost burden to add to very tight budget for most small business. Failure to have the CMMC will cost even more.

Cost of Not Having CMMC
While unknown as of today, what has been communicated to the entire Defense Industrial Base, is that if you don't have the CMMC at the basic level, you will not be eligible for federal contracts. Many small businesses may not even be aware of this new requirement and that failure to obtain certification means ending contract work as a service provider to the Department of Defense. These companies will not be able to make employee payroll and the dream of having a meaningful business to take care of the business owner family could also end. Additionally, as a Prime contractor, it will be our responsibility to flow-down the requirements to our subcontractors. If the subcontractor does not have the certification, we would be required to end subcontractors contract agreement to remain in compliant with the DoD CMMC standards. Not having CMMC adds a tremendous cost and risk to any business but will disproportionately impact the small businesses.

Audit Imposters
I raise this subject as an awareness to inform the subcommittee. When the DoD presented the CMMC as the new way of life for all businesses within the Defense Industrial Base, many businesses ask a lot of questions of why, who will conduct the implementation and audits, how much, when will this happen, implications of if you don't have it, and many more questions. This started in Summer of 2019 before the pandemic and lockdown in 2020. Even before the CMMC Accreditation Body was formed, audit imposters, started advertising that they would certify your company as cyber compliant. The audit imposters have had no training and certainly not accredited by the CMMC Accreditation Body. Matter of Fact, the first set of Third-Party Assessor Organization or C3PAO auditors certified to perform audits was just issued in May 2021. The audit imposters are charging thousands of dollars to get a company ready and for many small businesses that are just now hearing about this, may in a moment of pandemic, and fear of losing their government contract, may fall prey to an audit imposter.

As I close, I recommend that subcommittee members closely monitor this very important implementation of the CMMC initiative. While I know there are so many other issues to focus on, CMMC has ramifications that reach far beyond what we can realize at this moment. It is important that

1. Cost is articulated clearly to reduce price gouging and to allow small businesses to plan; and that there is a balanced cost approach that does not reduce small business participation in the federal marketplace;
2. DoD continues to work closely with the various advocacy groups to ensure that the Defense Industrial Base contractors know that the Office of Small Business is aware of the implications of this new initiative; and
3. DoD and the Office of Small Business start as soon as possible to put various roadblocks in place to reduce the number of audit imposters.

Thank you for your time and addressing this very important subject that impacts thousands of small businesses that do business with the Department of Defense.

Testimony of

Michael Dunbar

President, Ryzhka International

On Behalf of
HUBZone Contractors National Council

House Committee on Small Business
Subcommittee on Oversight, Investigations, and Regulations

"CMMC Implementation: What It Means for Small Businesses"

June 24, 2021

Chair Phillips, Ranking Member Van Duyne and Members of the Subcommittee, thank you for the opportunity to testify before you today. My name is Michael Dunbar, and I am the President of Ryzhka International, LLC, located in Pompano Beach, Florida. Ryzhka International provides lubricants and fuel oil in both bulk and package quantities to the federal government, commercial and maritime industries. I am a proud service-disabled veteran-owned and HUBZone certified small business. I am also a member of the Secure Supply Chain Consortium.

I am testifying today on behalf of the HUBZone Contractors National Council, a non-profit trade association providing information and support for companies and professionals interested in the Small Business Administration's (SBA) HUBZone program. We would like to thank the Committee for its commitment to small businesses and for advancing policies that support small businesses doing business with the federal government. Thank you for highlighting this critical topic – the impact of the Cybersecurity Maturity Model Certification (CMMC) on small business contractors.

In a recent hearing in the Senate Armed Services Committee, Deputy Assistant Secretary of Defense of Industrial Policy Jesse Salazar said it best: "The Department's approach to cybersecurity must balance the need for accountability with a recognition of the challenges facing small businesses."[1] Small businesses understand the importance of cybersecurity resiliency and the very real threats facing their companies. According to the Department of Defense's (DoD) contracting data, 74% of the Defense Industrial Base (DIB) are small businesses.[2] Small businesses are not looking for some way to opt out or ignore this problem - instead they are seeking to comply with CMMC to secure their companies. However, as outlined below, small contractors face unique challenges that require urgent solutions.

Background

With the constantly evolving cybersecurity standards for government contractors, it can be challenging for small businesses to stay current and remain compliant. As federal agencies have made progress since the early 2000s in setting up information security programs across government, these programs remain unable to keep up with growing cybersecurity threats. The government continues to seek a cybersecurity strategy for contractors that is cohesive, with standards and processes that are not duplicative and are worth the investment. To tackle this growing problem, the DoD created a new certification – the Cybersecurity Maturity Model Certification (CMMC).

The certification ecosystem can be equated to an onion – the outside layer is the DoD, which came up with the CMMC Model v1.02[3] and lays out the maturity processes and cybersecurity best

---

[1] *Cybersecurity of the Defense Industrial Base, Hearing before the Subcomm. on Cybersecurity of the S. Comm. on Armed Services,* 117th Cong. (2021) (statement of Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy).

[2] *Cybersecurity of the Defense Industrial Base, Hearing before the Subcomm. on Cybersecurity of the S. Comm. on Armed Services,* 117th Cong. (2021)

[3] Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC., CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) Version 1.02, March 18, 2020. Available online at: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

practices utilized in the framework.[4] The CMMC Accreditation Body (AB) is the next layer, which has a MOU with DoD and is tasked with creating and overseeing the certification process that adheres to the Model v1.02 standards. The third layer is the Certified Third-Party Assessment Organizations (C3PAOs), which are organizations overseen by the AB to schedule assessments, review and submit completed assessments for certification by the CMMC-AB. Within the C3PAOs are certified assessors. They are trained by the C3PAOs to provide certified assessment and consultative services to the organizations seeking certification (OSCs) – the federal contractors that do business with the DoD.

Despite the challenges presented by the pandemic, the CMMC rollout has remained fairly on schedule. In September 2020, the first provisional assessors were trained – 73 were tasked with performing mock assessments to be able to give feedback to the AB and DoD. According to the AB's published timeline,[5] certified training will continue to happen this year with commercial assessments available starting in the winter of 2021. While the DoD has said that all contractors will need to be certified by 2025, prior to October 1, 2025, the published DFARS rule impacts certain large and small businesses that are competing on acquisitions that specify a requirement for CMMC in the statement of work. According to the rule, these businesses will be required to have the stated CMMC certification level at the time of contract award. Inclusion of a CMMC requirement in a solicitation during this time must be approved by the DoD and it is estimated that 129,810 companies will pursue their CMMC certification during the initial 5-year period. By October 1, 2025, all entities receiving DoD contracts and orders, other than contracts or orders exclusively for commercially available off-the-shelf items or those valued at or below the micro-purchase threshold, will be required to have the CMMC level identified in the solicitation. At minimum this will be a CMMC Level 1 certification. CMMC certifications are valid for 3 years; therefore, all businesses will be required to renew their certification every 3 years.[6]

The federal government has long identified the need to safeguard sensitive information and understands that cybersecurity is a dynamic issue. Small businesses, however, are experts on the goods and services they provide. As such, they do their best to focus on supplying a product, making a profit, and retaining employees. Most small business owners are not IT professionals or cybersecurity specialists themselves. Therefore, they must seek outside assistance to understand CMMC, get ready for certification, apply, and maintain proper cybersecurity. The Council makes the following recommendations to improve the rollout of CMMC to maintain a strong industrial base:

Recommendations

1. **Increase cost transparency and put guardrails on rising compliance costs for small businesses.**

[4] Previous iterations of the CMMC model can be found on the Office of the Under Secretary of Defense for Acquisition & Sustainment CMMC website at: https://www.acq.osd.mil/cmmc/draft.html.
[5] CMMC Accreditation Body Path to an Accreditation Ecosystem, https://mcusercontent.com/6e7d7963b1219eb1b0fbda703/files/543677c7-9ead-4f47-b865-e92f0df4af8c/Accreditation_Ecosystem.pdf.
[6] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 FR 61505 (published September 29, 2020).

One of the biggest frustrations for small businesses throughout the rollout of the certification has been cost transparency. Some small businesses have estimated costs upwards of $100,000 to prepare for a Level 3 certification. Although small businesses were referenced many times in the recent DFARS rule, there is no information on how the DoD will account for the impact compliance will have on the Defense Industrial Base. The recently effective CMMC DFARS rule[7] outlined unrealistic cost estimates for firms to score their compliance with NIST 800-171. The rule estimated that for a basic assessment the average contractor would spend a total of $75, with just under $50 and another $25 to put the information on the Supplier Performance Risk System (SPRS) portal. This low dollar amount completely underestimates the cost that it will take for contractors to complete these reviews successfully. The DoD should engage industry more broadly to understand the new costs being incurred by contractors during this phase of CMMC implementation.

The initial cost to start my business was less than $1,000 – I have estimated that to comply with CMMC Level 3 and the ongoing costs, it would be closer to $100,000. A common reply to a concern around these costs is "if you can't afford the cost, then maybe you shouldn't be selling to the government." However, small businesses are caught in a cycle of being unable to afford to put the security requirements in place without a government contract, yet these systems must be in place to bid on them. Many businesses have spent tens of thousands of dollars to get "CMMC ready," even though many unknowns remain. Some industry estimates[8] for a Level 3 certification show that a small business with 10 employees can expect to pay roughly $77,000 in professional services, not including hardware purchases for additional IT support, as well as approximately $2,000 per month in ongoing service fees. That equates to about $10,000 per employee. A 200-person company can expect to pay roughly $148,000 in professional services to get set up for CMMC Level 3 or NIST 800-171, not including hardware purchases for additional IT support and approximately $26,000 per month in ongoing monthly service fees. This is roughly $2,500 per employee.

The smallest businesses in the Defense Industrial Base are disproportionately impacted by the costs associated with cybersecurity compliance. Many companies do not have dedicated staff in place to handle cybersecurity or any IT related issues. Therefore, these services must be outsourced. In the case of CMMC, small businesses have had to hire someone to write the policies and procedures, train employees, purchase services, software and additional technology needed to comply with the appropriate CMMC level, pay for an audit and hire a professional to be present to oversee the auditor. These costs do not factor in ongoing compliance costs.

Further, it has been challenging for all sizes of business to predict the costs for the actual CMMC audit. It is difficult to predict how many auditor-days will be needed that will in turn determine if an assessment will cost $5,000 or $100,000. C3PAO's can charge any amount they choose, without any scaling for business size or guidance from the government on fair pricing. This injects even more uncertainty for small businesses. The Council recommends that the government put

[7] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 FR 61505 (published September 29, 2020).
[8] *Estimates provided by Trusted Internet, LLC.*

guardrails in place for private auditors with respect to for how much small businesses can be charged for these assessments.

2. Establish clear communication on CMMC efforts.

A lack of transparency and clear, consistent communication by DoD in the rollout of CMMC and its implementation by the CMMC Accreditation Body has been concerning. Critical information has been communicated inconsistently and often via social media platforms like LinkedIn. The Council suggests putting together a more clear, consistent delivery of information through a central government platform or website.

The DoD should also establish a method for continual feedback and seek to incorporate industry feedback throughout CMMC implementation. So far it has been challenging for industry to communicate with the DoD about best practices or ideas for implementation. Additionally, streamlined communication is needed to ensure consistency in Department-wide CMMC implementation. It is imperative that government officials across the DoD (and eventually civilian agencies) receive consistent, adequate training on implementing CMMC requirements. Issuing formal, department-wide instructions, guidance and frequently asked questions will help the government implement CMMC consistency.

There has also been confusion around communication regarding reimbursable costs. DoD officials have stated during speaking engagements that costs to become ready to get certified could be reimbursable to manufacturers. However, there is no clarity about any reimbursement for non-manufacturers or if this will be the case. Further, it is unclear if there will be any mechanism for businesses to recover any costs if they bid on the solicitation but are not awarded the contract. Since a company must be CMMC certified at a certain level just to bid, the Council suggests offering small businesses grants to help cover some of these costs.

Due to the COVID-19 pandemic, many small businesses employees are working from home. As a result, it remains unclear if employees are subject to home audits to comply with CMMC. There has been conflicting information about this issue, with a member of the CMMC-AB stating that there will be home audits. There has, however, been no official announcement. Currently, the CMMC assessment guide does not consider telework – there is no guidance on this issue. The Council believes clarity on this issue is important, considering it will add significant cost and implementation barriers for small businesses.

3. Streamline new and existing standards for contractors.

The federal government lacks unified cybersecurity standards across all agencies. Contractors have had to grapple with how and when to comply with NIST 800-171, DFARS 252.204-7012 and many others. For example, the Department of Energy (DOE) has its own cybersecurity program - Cybersecurity Capability Maturity Model (C2M2).[9] Finalized in 2014, the C2M2 "is a U.S.

[9] CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) Version 1.1 (February 2014), https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

Department of Energy (DOE) program that enables organizations to voluntarily measure the maturity of their cybersecurity capabilities in a consistent manner."[10]

DOE states that the C2M2 was developed from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.0 by removing sector-specific references and terminology. The ES-C2M2 was developed in support of a White House initiative led by the DOE, in partnership with the Department of Homeland Security (DHS), and in collaboration with private- and public-sector experts.[11] Companies that do business with multiple federal agencies will have to continue to comply with each unique Department's cybersecurity assessments and standards. Cost is also problematic with regards to this issue. For example, I am currently a prime or subcontractor at the DoD, Department of Commerce, Department of Homeland Security, Department of Veterans Affairs, and Department of Transportation. It is important to my business and success of my federal contracts that I am compliant with each Department's standards. The Council encourages federal agencies to work together to ensure a level of standardization when adopting CMMC or providing reciprocity across government departments.

An additional mechanism that would ensure more effective implementation is to allow companies to have a Plan of Action and Milestones (POA&M) after a CMMC assessment. Currently, CMMC certification is an all or nothing process – if an assessor determines your company is at a Level 2 because of only a few factors, there is no way to make the necessary changes and achieve a Level 3 certification. Further, there is no dispute mechanism for companies to challenge a given certification level. This is problematic because assessments are subjective, and companies should have the ability to use a resolution process to settle CMMC assessment disputes, especially small businesses.

It is encouraging that DoD has recently committed that as part of the CMMC certification process, the Department will deconflict and streamline multiple cybersecurity requirements to prevent duplicative assessments. This includes providing clear guidance on the alignment of the NIST SP 800-171, DoD Assessment Methodology and CMMC, as they pertain to safeguarding controlled unclassified information (CUI), as well as the requirements and assessment approach for contractors that use cloud service provider offerings. The Council encourages DoD to work closely with industry - particularly small businesses - to streamline these requirements.

4. Create a system for proper oversight and an equitable rollout.

A looming question that remains in the minds of contractors is the order in which the Defense Industrial Base will get certified. With over 300,000 companies – or even the DoD estimated 129,810 companies – that will pursue their initial CMMC certification during the initial five-year period, how will this get accomplished? Creating a streamlined system to put companies in the queue to be certified will be crucial to the successful execution of this program. Many small businesses worry that they will be put at the back of the line and face massive delays. As numerous companies also serve as subcontractors, an equitable rollout is imperative to these companies.

---

[10] Office of Cybersecurity, Energy Security, and Emergency Response, C2M2 Model v2.0 Update – Invitation to Participate, https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program.

[11] Id.

The DoD has also provided industry with multiple, conflicting answers on how the certification will apply to subcontractors, and more importantly, how the CMMC level of subcontract work will be determined. In DFARS rule[12] effective last fall implementing the framework, it states that the CMMC requirements must be included in all subcontracts, as well as "other contractual instruments." Therefore, all non-commercially available off the shelf (COTS) contracts, prime and subcontractors performing the covered contracts are required to be certified. The DoD has stated in the past that the pieces of subcontracting work with requirements for a certain CMMC level will be determined through the program office in conjunction with the prime contractor. However, depending on its role, a subcontractor may not have to access the CUI. It is also possible that this is no longer the case – there is a lack of clear communication on this issue. Therefore, it is unrealistic to require all subcontractors to get certified – the cost for small businesses is too high for a certification they will not need.

Another concern centers around assigning certification levels for both the government and prime contractors. Training for the acquisition workforce on how to properly assign levels to contracts/industries without overinflating them is crucial. Currently, consultants and companies are just guessing at which industries are going to "probably" be a Level 1 or 3. I think we can all agree that this presents a real problem for small businesses. For example, for my industry, I have been informed that DOE has suggested that fuel should be a Level 4 certification. That would be devastating to my company because the cost of getting Level 4 certified would likely be many times the cost of Level 3. If small fuel suppliers walked away from the work because of the cost of certification requirements, the fuel supply industry would be crippled. With fewer suppliers, fuel costs to the government could increase by up to 50 percent.

Further, it is important that prime contractors adequately assess the proper level of certification as well. A fear for subcontractors is that a prime will determine that a minimum of CMMC Level 3 is required for all subcontractors, regardless of contract, to provide a blanket safeguard. This would place an undue burden on subcontractors to meet CMMC levels that do not correspond to the products or services they provide. A mechanism to resolve disagreements between the prime and subcontractor on the recommended certification is necessary.

In conclusion, the CMMC needs to be adapted to secure the Defense Industrial Base without alienating small businesses. The federal government has a long and complex history of governing cybersecurity regulations and compliance among its contractors. A streamlined approach needs to be taken for contractors to navigate all of these standards and systems to successfully secure the Defense Industrial Base. Thank you for the opportunity to testify today and I look forward to answering any questions.

[12] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 FR 61505 (published September 29, 2020).

HO-CHUNK INCORPORATED

1 Mission Drive • Box 390
Winnebago, NE 68071
800.439.7008
402.878.2809
www.hochunkinc.com

VIA EMAIL TO: Lauren.Finks@mail.house.gov, **cc:** Irene.Rivera@mail.house.gov

July 1, 2021

The Honorable Dean Phillips, Chairman
The Honorable Beth Van Duyne, Ranking Member
Subcommittee on Oversight, Investigations, and Regulations
Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Phillips:

On behalf of Ho-Chunk Inc. (Ho-Chunk), I am pleased to submit the following comments and recommendations in response to the hearing held on June 24, 2021, by the U.S. Committee on Small Business' Subcommittee on Oversight, Investigations, and Regulations entitle "CMMC Implementation: What It Means for Small Businesses." We would like to thank you, Ranking Member Van Duyne, and other members of the Subcommittee for carefully considering the concerns and impact the Department of Defense (DoD)'s Cybersecurity Maturity Model Certification (CMMC) requirements and implementation have on the small businesses that comprise a significant portion of the defense industrial base (DIB).

Ho-Chunk, Inc. is a parent company to tribally-owned government contractor subsidiaries providing economic development to the Winnebago Tribe of Nebraska. As a parent company of small businesses supporting critical missions of various U.S. government customers, our goal is to provide quality services within our capabilities in federal contracting. Ho-Chunk, Inc. as well as the majority of the defense industrial base, understands that protecting the data received from our government customers is critical and that there are foreign adversaries who pose a risk to that data on a daily basis. We do not disagree that robust cyber hygiene is necessary, however, as a small business we have concerns regarding the costs, processes, and timeline for that compliance to CMMC standards.

I. Introduction and Background

As the single largest category of the federal government's discretionary spending, DoD prime contract awards represent a significant portion of all federal contract awards to small businesses. However, entering the federal supply chain has always been a lengthy and arduous process for most small businesses and CMMC is making that process even more difficult and expensive. CMMC creates a barrier to entry into government contracting for small businesses, both from a regulatory and cost consideration. Companies must be CMMC compliant upon contract award and there are significant costs to that compliance.

Small businesses are a critical part of the defense supply chain. CMMC will diminish the opportunities for small businesses to participate in government contracting unless changes are made to the current implementation process. Many small businesses will have no choice but to walk away from DoD contracts that have CMMC requirements. According to a 2019 Bloomberg report, the Federal supplier base had a 32% decline of small federal contractors working on unclassified prime contracts from 2009 to 2018. This was compared to a 4% decline for large vendors during that same time period.[1] This data shows that only large vendors are currently able to meet the CMMC standards in a timely manner, and DoD needs to provide additional assistance to small business to reverse the decline.

The purpose of CMMC is to standardize cybersecurity practices across the Federal government defense industrial base and to ensure that organizations who handle Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) are able to adequately safeguard that data. There are five levels of certification ranging from 1 (lowest) to 5 (highest). There is a significant cost difference in getting from Level 1 to Level 3 compliance, and even more so to Levels 4 and 5.

DoD released the CMMC version 1.0 on January 31, 2020 and issued an interim rule that was effective on November 30, 2020. This interim rule phased in the rollout of CMMC and caused many questions and concerns from both large and small companies. All contracts over the micro-purchase threshold (except for commercial off-the-shelf items) will require CMMC beginning September 30, 2025. "In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level."[2] Previously, DIB contractors were responsible for implementing, monitoring, and certifying the security of their IT systems and any sensitive DoD information stored on or transmitted by those systems. CMMC will require third-party assessment of contractors' compliance with CMMC practices, procedures, and capabilities.

Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements (below), is currently prescribed for use in all solicitations and contracts or task orders or delivery orders, excluding those exclusively for the acquisition of COTS items. This DFARS clause requires a contractor to have the requisite CMMC level *at the time of contract award*, maintain that level for the duration of the contract and ensure that its subcontractors also have the appropriate CMMC level *prior to awarding* a subcontract or other contractual instruments. The Prime contractor must also include the requirements of the clause in all subcontracts or other contractual instruments.

DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements.

As prescribed in 204.7503(a) and (b), insert the following clause:

CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENTS (NOV 2020)

---

[1] Murphy, Paul. "Federal Supplier Base Continued to Shrink in Fiscal 2018", Bloomberg Law, Bloomberg L.P. May 23, 2019. Web June 26, 2019.

[2] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041) issued Sept 29, 2020.

(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html).

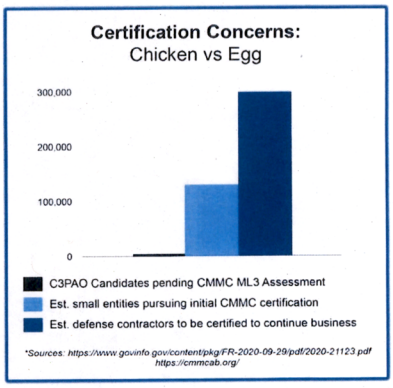
(b) *Requirements.* The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts.* The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

In fiscal year 2019, DoD awarded more than $75 billion in prime contracts to small businesses.[3] All companies in the defense industrial base, whether large or small, Prime or subcontractor, will need some level of CMMC certification to be eligible to continue supporting DoD.



DoD has made it clear that all companies doing business will need to be, at a minimum, Level 1 certified. If CUI is processed, then Level 3 will be required. According to the CMMC Accreditation Body (CMMC-AB), they estimate there will need to be assessments for 300,000+ companies in the DoD supply chain.[4] Since all legal entities, including joint ventures and the individual parties to the JV, as well as subcontractors, that participate in a contract with CMMC requirements (level 1 and above), must be assessed[5], that number will most likely be higher than 300,000. That is a significant number of assessments that need to be performed in a short period of time

[3] Department of Defense, Office of Small Business Programs, "Guide to Marketing to DoD". "Target Your Market." Marketing to DoD (defense.gov). June 3, 2021.

[4] CMMC Accreditation Body. "CMMC-AB is accountable for delivering". CMMC-AB website

https://cmmcab.org/board-of-directors.

[5] CMMC-AB website FAQ (cmmcab.org)

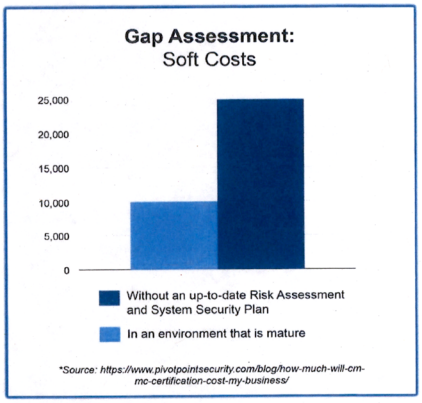
and the current CMMC implementation process does not have adequate guideposts to ensure this will happen. If timely assistance and assessments are not provided to small businesses, they will essentially be cut out of DoD contracts and subcontracts for the foreseeable future. We do not believe this is what Congress intended when it enacted the CMMC requirement.

II. Obstacles to Small Business Implementation of CMMC

One of the primary concerns Ho-Chunk, Inc. has with the current CMMC implementation process is with statements by the DoD that seem to imply that Prime contractors will be responsible for CMMC requirements. These statements assume that all Prime contractors are large companies with significant resources; but that is not the case, as many small businesses like Ho-Chunk, Inc. and its subsidiaries serve as Prime and subcontractors. We believe the reason for this significant misunderstanding of the impacts of CMMC is due to the fact that very few small businesses are involved in the planning and implementation strategies for CMMC. As stated above, there many small businesses working with DoD as Prime contractors, and for the most part they are struggling with implementing CMMC requirements and not be consulted on about how to improve implementation.

For example, to date, Ho-Chunk, Inc. and its subsidiaries have spent $1,000,000 to $1,500,000 to comply with the NIST 800-171 and to prepare for CMMC certification. We expect the ongoing costs to be close to $1 million a year as well, not counting the actual certification costs. Most small companies cannot make that type of investment up front when it is not clear what the standards for certification will be. For ourselves, we think we are investing in the right equipment, software, policies, and procedures, but we don't know what the objective standards will be for the audit. And, we don't know when we will be able to schedule an audit, or if an auditor will even be available.

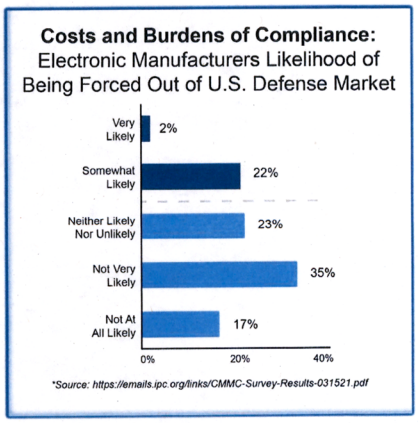
That uncertainty as to costs, process, or even the timeline is one of the larger problems with the implementation plans for CMMC. There are also concerns with "requirements creep" from the government agency in that will they require Level 3, or even higher for contracts containing CUI, when that level is not necessarily required by the CMMC. There has been no guidance from DoD in how to determine the appropriate level of certification.



Small business Prime contractors themselves will need training to understand what level will be necessary for their subcontractors to receive contract information. Although the DFARs requirement states that the Prime contractor will "ensure" that the subcontractor has a current CMMC certificate, there is no guidance as to how Prime contractors will determine the level to request from their subcontractors.

This uncertainty about what the reality of CMMC will be is adversely affecting the defense industrial base small businesses.

In an industry survey and report from new IPC, a global association for electronics manufacturers, the foreword to the report states, "(t)his report, drawing on IPC industry survey results, amplifies concerns that the CMMC may weaken U.S. industrial base resiliency even as it seeks to bolster security for those that



remain in it."[6] According to the report, one-quarter (24 percent) of electronic manufacturers say the costs and burdens of compliance with CMMC may force them out of the DoD supply chain.[7]

To date there is only one CMMC third-party assessor organization certified as a C3PAO. Combine that with the estimated more than 300,000 contractors in the DIB and you can understand our concerns. Taking into account that each of these contractors must hire a C3PAO to inspect and verify the required cyber standards from Level 1 to Level 5, there will not be enough auditors to ensure compliance even with the September 2025 timeline.

III. Suggested Compromises to Small Business CMMC concerns

Ho-chunk, Inc. is the parent company to a number of subsidiaries who work with the federal government, and we understand why cybersecurity protection is so important. The work of Ho-Chunk, Inc. and its subsidiaries has been consistently recognized for excellence in operations and honored for its work in federal government contracting. Significant awards include recognition as the Minority Business Development Agency Advocate of the Year from the Department of Commerce, the Small Business Prime Contractor of the Year from the U.S. Department of State, Secretary's award for Excellence in Small Business Contracting from the U.S. Department of State, and the SBA's Minority Small Business Person of the Year was awarded to CEO Lance Morgan.

These awards are indicative of the high standards, accomplishments and capacity of Ho-Chunk, Inc. to receive and carry out contracts that meet the needs of the federal government – both domestically and internationally – and highlight how this type of business can succeed and thrive in Indian Country. All with the goal and mission of improving the lives of tribal citizens and providing tribal governments with the tools they need to strive for self-sufficiency.

All Native Group (ANG) is Ho-Chunk's largest division, comprised of a network of small businesses that support the critical missions of various U.S. government customers. ANG specializes in information technology (IT), telecommunications, health, logistics, specialized training and other professional services in the government sector and supports a breadth of government agencies. These agencies include the Department of Defense, Department of State, Department of Labor, Department of the Interior, Commerce Department, General Services Administration, U.S. Strategic Command, Defense Threat Reduction Agency, NASA, Department of Homeland Security and the U.S. Navy, Air Force and Army. ANG has support offices in Fairfax, Virginia and satellite offices in Colorado Springs, Colorado, and Huntsville, Alabama. In addition to providing a range of government services, ANG offers training and job opportunities for Native Americans in the government sector.

As a sampling of some of their accomplishments, the company was selected to provide information technology and cyber security support for the U.S. Army's Network Enterprise Technology Command supporting the command's operations around the globe. ANG was also contracted to provide support to the Defense Health Agency (DHA), Solutions Delivery Division (SDD) to

[6] IPC. "Strengthening National Security and Supply Chain Resiliency by Improving DoD Cybersecurity Certification." June 2021.

[7] IPC. June 2021. CMMC Survey Results_031521 (ipc.org)

establish effective cybersecurity for a variety of systems under the DHA umbrella. ANG's Colorado office is the latest move for the company as it expands its reach and expertise in the government IT and cybersecurity space.

Flatwater Group (Flatwater) is a collection of companies that provide a range of products and services for government and commercial clients. Business lines include professional services, business technology solutions, interior furnishing and design, healthcare solutions, metal products, transportation and logistics. Flatwater supports a range of government clients, including Department of the Interior, Defense Logistics Agency, Department of Commerce, Department of the Treasury, the Department of Health and Human Services and numerous others.

This extensive experience with government contracting and handling Federal Contract Information, as well as classified and unclassified information, gives Ho-Chunk, Inc. and its subsidiaries the experience necessary to recognize when a regulatory change will have an adverse impact on its operations and its customers, and on similarly situated small businesses.

Ho-Chunk, Inc. would like to recommend to the Subcommittee several compromises in the implementation for CMMC:

- We would like to recommend an 18-month extension of the deadline for requiring all DIB contractors to be certified. This extension would allow more C3PAOs to be certified, which would provide more auditors to perform the assessments.
- We would recommend that DoD continue to allow for self-certification by contractors, at least for Levels 1 through Level 3 for two more years. This would allow the focus to be on the higher Levels 4 & 5 for the data that is most at risk and allow the few auditors available to focus on those higher level requirements.
- Require that DoD issue a clear written policy on the scope of assessments. More regular, official communication is needed from DoD and the CMMC Accrediting Body with small businesses who contract with the federal government about the requirements and policies of CMMC.
- Training for small businesses on what is required for CMMC compliance, or specifically in a CMMC audit is needed. The Small Business Administration (SBA) could assist with that training if funding could be provided either from DoD, or Congress. SBA has the contacts with the small business community and already provides extensive training for these businesses.
- Monetary assistance to small businesses to implement CMMC requirements. This could take the form of reimbursement on contracts that contain the clause as in a separate contract line item number specifically for CMMC costs, or grants to implement CMMC requirements. The grants could be administered through the SBA as they have proven they can implement large scale contacts to small businesses.
- Carefully consider why the additional requirements were added to the existing NIST SP 800-171 to create the CMMC framework.

- Most importantly, we believe Congress needs to direct that a study be performed to determine the impact of CMMC implementation on small businesses. The subcommittee's hearing is a good start, but there are significant impacts of CMMC implementation on small businesses that Congress is unaware of and we believe a congressionally-directed study will help educate and advise Congress and the DoD on how best to alleviate the burdens of CMMC on small businesses and ensure that they remain a significant component of the DIB.

- DoD issued a Dear Tribal Leader Letter (DTLL) on February 9, 2021, requesting input into the DoD Plan of Action to implement President Biden's Presidential Memorandum, *Tribal Consultation and Strengthening Nation-to-Nation Relationships* and Executive Order 13175, Consultation and Coordination with Indian Tribal Governments. Ho-Chunk, Inc. submitted comments to that DTLL and requested that DoD hold tribal consultations on important subjects that impacted tribes and tribally owned businesses that worked with DoD. We focused our comments on the section entitled "Communicate with Tribes and Tribal-owned businesses about opportunities to work with the Department" and specifically detailed the issues and concerns we have with CMMC implementation. We reiterate our call for DoD to hold tribal consultations as part of its regular communication strategy to small businesses on CMMC implementation and ask that the Subcommittee support this request and inform DoD of your support.

IV. Conclusion

We hope that our comments and recommendations are helpful in the Subcommittee's consideration of the impact of CMMC on the small businesses in the defense supply chain, and as always, we are available for any discussion. Please do not hesitate to contact us if you would like any further information.

Sincerely,

Annette Hamilton

Annette Hamilton

COO - Ho-Chunk, Inc.

IPC

BUILD ELECTRONICS BETTER

STRENGTHENING NATIONAL SECURITY AND SUPPLY CHAIN RESILIENCY BY IMPROVING DOD CYBERSECURITY CERTIFICATION

An IPC Report — June 2021

TABLE OF CONTENTS

FOREWORD

Cyberattacks on the U.S. industrial base continue to grow in number, scope, and sophistication. U.S. electronics manufacturers are especially attractive to attackers given the unique importance of electronics in nearly all defense applications and weaponry. In response, the industry has taken proactive steps to protect controlled unclassified information (CUI) and other sensitive information related to the design, production, and performance of defense electronics.

The most notable example of the industry's proactive posture is the development of the IPC-1791 "Trusted Supplier" standard and the corresponding Qualified Manufacturers List (QML) for those that design and fabricate printed circuit boards and printed circuit assemblies. The standard, which was developed in collaboration with the U.S. Defense Department's Executive Agent for Printed Circuit Boards and Interconnect Technology, builds on previously existing standards to cover both cyber and physical security. More and more companies are getting validated to the standard, establishing a more robust community of trusted suppliers of electronics to the Department of Defense (DoD).

IPC-1791 anticipated the Cybersecurity Maturity Model Certification (CMMC). Those companies that are validated to IPC-1791, in fact, are better prepared to achieve the requisite certification under CMMC. However, the CMMC places significant new obligations on electronics manufacturers, who tend to operate on razor-thin margins in a highly competitive global marketplace. Defense-related work is usually a small percentage of overall revenue for these businesses, raising concerns for many companies about whether the higher-than-expected costs of CMMC compliance can be justified.

This report, drawing on IPC industry survey results, amplifies concerns that the CMMC may weaken U.S. industrial base resiliency even as it seeks to bolster security for those that remain in it. The report's author, defense cyber policy expert Leslie Weinstein of HITRUST, lends her analysis of the survey results and offers opportunities for DoD to better support the industry through CMMC compliance and certification.

IPC will continue to be an advocate for the industry on this important issue and encourages companies to take all necessary steps to understand the CMMC and seek certification as necessary.

John W. Mitchell
President and CEO
IPC

EXECUTIVE SUMMARY

This report finds:

- The costs and burdens anticipated to be necessary to achieve Cybersecurity Maturity Model Certification (CMMC) compliance will drive many suppliers out of the U.S. Department of Defense (DoD) supply chain, which will negatively impact national security.
  - Nearly one-quarter (24 percent) of IPC survey respondents indicate that the costs and burdens of CMMC compliance will likely force them out of the DoD supply chain.
  - A third (33 percent) of respondents feel the CMMC will weaken at least part of the electronics industrial base, while 18 percent are unsure, highlighting the uncertainty around CMMC.
  - Roughly 41 percent of respondents believe that applying the CMMC clause to their suppliers will create problems within the supply chain.
- DoD underestimates the cost impact of the Defense Federal Acquisition Regulation Supplement (DFARS) interim rule, which is premised on a false understanding that the cost burden on the U.S. defense industrial base (DIB) is manageable and sustainable.
  - Approximately 68 percent of respondents foresee the need to hire a consultant or bring in outside help to prepare for CMMC assessment.
  - Nearly one-third (32 percent) report it will take one to two years to prepare to undergo a CMMC assessment.
- Most companies seem unaware of the potentially heavy costs associated with CMMC compliance, and the DoD has provided too few resources to ensure the DIB can achieve CMMC compliance.
  - Less than half (49 percent) of survey respondents feel they are "very" or "extremely" familiar with CMMC compliance.
  - Some 52 percent of respondents report that DoD has not provided industry with sufficient guidance to support CMMC preparedness efforts.
- The DoD should leverage existing standards to help reduce the costs and burdens of CMMC compliance.
  - While the CMMC's stated objective is to improve supply chain visibility and monitoring, it does so at the expense of other key aspects of supply chain health. The CMMC runs the risk of creating barriers to entry which will complicate supplier onboarding and reduce supply chain diversity and resiliency.

INTRODUCTION

Last year, the U.S. Department of Defense (DoD) issued an interim rule establishing a new framework for strengthening the cybersecurity posture of the U.S. defense industrial base (DIB). Referred to as the Cybersecurity Maturity Model Certification (CMMC), the framework sets out new requirements, as well as an assessment and certification process, that is designed to better safeguard sensitive federal contract information (FCI) and controlled unclassified information (CUI). When it is fully implemented, the CMMC will place new obligations on all U.S. electronics manufacturers that directly or indirectly serve the U.S. defense market.

The CMMC is a laudable and necessary DoD initiative, but it is not without risk to the resiliency of the DIB. In creating the CMMC, DoD has failed to appreciate the true costs associated with certification. The costs, in fact, are considerable, especially for electronics manufacturers which operate in a highly competitive, thin-margin business. Given that DoD-related sales are a small percentage of overall sales for most electronics manufacturers, many may exit the defense market, concluding that CMMC costs cannot be justified.

To better understand the potential impact of the CMMC on U.S. electronics manufacturers, IPC fielded an industry survey between February 25 and March 5, 2021. The survey garnered 108 responses from contract manufacturers, printed circuit board fabricators, original equipment manufacturers and suppliers that self-reported they are planning to undergo a CMMC assessment in the next five years.

The results of the survey confirm the likelihood that the CMMC will push many companies out of the defense market unless DoD takes steps to support the industry's assessment and compliance. Even more worrisome, the risk to industrial base resiliency may be greater than currently realized as most companies are not fully aware of the heavy costs associated with CMMC compliance.

This report concludes that the DoD should reduce the costs and burdens of the CMMC on the DIB by leveraging existing industry standards and certifications. There are several widely adopted security standards and certification processes that have been implemented by thousands of companies around the world. Recognizing additional certifications currently available in the market will not only save DIB companies money and reduce the number of redundant audits by leveraging their existing certifications, but it will also create a pool of DIB companies who are able to bid on solicitations containing the CMMC Defense Federal Acquisition Regulation Supplement (DFARS) clause.

CMMC DFARS INTERIM RULE OVERVIEW

On September 29, 2020, the DoD published an emergency interim rule in the Federal Register to amend the DFARS to implement a DoD Assessment Methodology and the CMMC framework to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. The CMMC requires a third-party verification of contractor implementation of cybersecurity requirements and has a five-year implementation timeline. The DoD assessment and scoring methodology measures contractor implementation of existing cybersecurity requirements. The existing cybersecurity requirements, found in the DFARS clause 252.204-7012, requires contractors who handle CUI to implement NIST SP 800-171 in their environments which handle CUI. However, findings from a DoD Inspector General report (DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicated that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI, and it recommended that DoD take steps to assess a contractor's ability to protect this information. The DFARS interim rule was issued in direct response to this finding and is meant to provide DoD visibility into the cybersecurity posture of its supply chain.

In addition to the DoD Assessment Methodology, the DFARS interim rule introduced three new DFARS Clauses:

- 7019 Clause: Requires contractors who handle CUI to implement NIST SP 800-171 for environments which handle CUI; conduct a self-assessment (Basic Assessment) using NIST SP 800-171A1A[1] and the DoD Assessment Methodology scoring rubric; and submit their score into the Supplier Performance Risk System (SPRS) to be considered for award with a contract containing both the -7012 and -7019 Clauses. The -7019 Clause has a three-year implementation timeline, with 100% of new RFPs to contain the clause by October 1, 2023. The score on record must not be more than three years old.
- 7020 Clause: Paired with the -7012 and -7019 Clauses, it requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level assessment, known as Medium and High Assessments.
  - Medium Assessment: Required for certain DoD awardees. The contractor provides DoD access to its facilities and personnel, if necessary, and prepares for/participates in the assessment conducted by the DoD. The DoD assessor will review the system security plan description of how each requirement is met and will identify any descriptions that may not properly address the security requirements. DoD will post the results in SPRS.

[1]Ross, Dempsey, and Pillitteri, U.S. National Institute of Standards and Technology (NIST), "Assessing Security Requirements for Controlled Unclassified Information," NIST Special Publication 800-171A, June 2018.

- High Assessment: Required for certain DoD awardees. The contractor provides the DoD access to its facilities, systems, and personnel and prepares for/participates in the assessment conducted by DoD. The DoD assessors will review the system security plan description of how each requirement is met and the contractor will demonstrate the implementation to the DoD assessors. DoD will post the results in SPRS.

- 7020 Clause: The CMMC clause. It is prescribed for use in solicitations and contracts, including solicitations and contracts using FAR Part 12 procedures for the acquisition of commercial items, excluding acquisitions exclusively for COTS items. CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, starting on or after October 1, 2025. CMMC certification requirements are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each subcontractor.

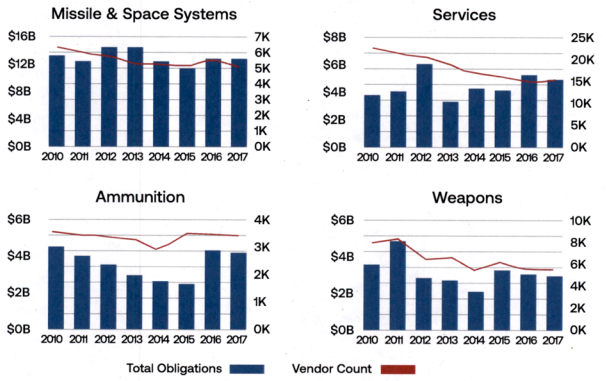
This white paper provides an analysis of an IPC industry survey and compares the findings with the DFARS Interim Rule's analysis of the impact of the CMMC to industry, highlighting major discrepancies that have the potential to detrimentally impact the DIB and ultimately undermine national security.

THE CMMC MAY CAUSE FURTHER EROSION OF THE DIB AND UNDERMINE NATIONAL SECURITY

The 2018 National Security Strategy "highlights the importance of a vibrant manufacturing sector to comprehensive national power, while warning of the dangers inherent in the weakening of America's manufacturing base: A healthy defense industrial base is a critical element of U.S. power and the National Security Innovation Base."[2] According to Dun & Bradstreet, the four characteristics of a healthy supply chain are supplier diversity, supply chain visibility, effective supplier onboarding, and supply chain monitoring.[3] While the CMMC's stated objective is to improve supply chain visibility and monitoring, the CMMC does so at the expense of other key aspects of supply chain health. The CMMC creates barriers to entry which complicate supplier onboarding and decrease supplier diversity, therefore reducing supply chain resiliency. Since 2010, critical manufacturing and DIB manufacturing industries have seen fluctuations in federal obligations spending, creating variability in vendor counts, and deteriorating DoD's supply chain (Figure 1). The effects of sequestration and the budget caps accelerated the downward trend in vendor counts, resulting in an estimated 20% decline in the number of prime vendors.[4]

[2] U.S. Dept. of Defense, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, September 2018, page 24. Hereafter cited as the "Defense Industrial Base Report."
[3] Brian Alster, Dun & Bradstreet Supply Chains Need Health Checks, Too, July 12, 2018
[4] US. Department of Defense, Defense Industrial Base Report, p. 26.

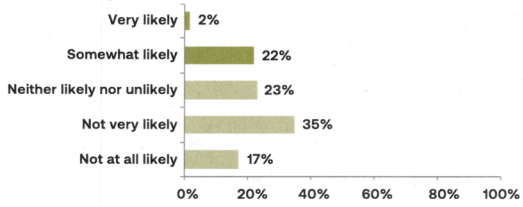
Figure 1: Falling Vendor Counts in Key Manufacturing and Defense Industrial Base Areas



Source: U.S. Department of Defense, Defense Industrial Base Report, p. 26.

Nearly one-quarter of the IPC CMMC survey respondents indicated that the costs and burdens of CMMC compliance are likely to force them out of the DoD supply chain (see Figure 2). Most of the survey respondents report that 50% or less of their annual company revenue comes from the DoD. For many small businesses, the costs and burdens of CMMC compliance may outweigh the benefits gained by supplying to the DoD. Respondents of the survey also indicated that the DoD has not done enough to prepare the DIB for the CMMC, noting a lack of sufficient guidance on the requirements. This lack of guidance on the requirements has created difficulties for the DIB in evaluating external resources, such as consultants, which 68% of respondents believe will be needed to prepare for the CMMC.

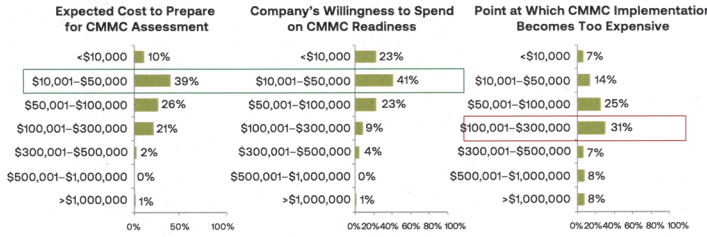
Figure 2: Likelihood of Being Forced Out of the U.S. Defense Market



Source: IPC Industry Survey, 2021

Most suppliers expect and are willing to spend upwards of $50,000 on CMMC readiness. At the same time, more than half of suppliers report implementation costs exceeding $100,000 would make CMMC readiness too expensive. In DoD's cost analysis submitted as supporting documentation with the DFARS interim rule, DoD estimated the cost of a CMMC Maturity Level 3 (ML3) certification to be more than $118,000 in the first year. Therefore, DoD's own cost analysis of CMMC ML3 compliance is in the range of being too expensive for 77% of IPC CMMC survey respondents. Figure 3 also highlights the apparent lack of awareness the DIB has of DoD's estimated cost of CMMC compliance.

Figure 3: Industry Willingness to Spend on CMMC Readiness



Source: IPC Industry Survey, 2021

The CMMC-Accreditation Body (CMMC-AB), the sole entity recognized by the DoD to issue CMMC certifications, created the concept of a "registered practitioner" (RP) and a "registered provider organization" (RPO). According to the CMMC-AB's website (cmmcab.org), "The RPOs and RPs in the CMMC ecosystem provide advice, consulting, and recommendations to their clients." RPs and RPOs are the "implementers" and consultants, but do not conduct Certified CMMC Assessments. These RPs "have attended CMMC-AB sponsored training classes, completed a test, signed the Code of Professional Conduct, and passed a criminal background check" prior to being listed on the CMMC-AB Marketplace. RPOs must "receive authorization from the CMMC-AB as a result of registering, sign the RPO agreement with the CMMC-AB, pass an Organizational Background Check via data provided to the CMMC-AB by Dun & Bradstreet and have a DUNS number, and at least one RP must be associated with the RPO at all times" to be listed on the Marketplace. The CMMC-AB's website further states that attaining the RPO badge simply means that a company has a "basic understanding of [the CMMC's] requirements" and does not connote expertise. The RP badge costs individual consultants $500 annually to maintain, and the RPO badge costs companies $5,000 annually to maintain.

While the preponderance of the IPC survey respondents claimed that DoD had not done enough to guide the DIB to qualified CMMC practitioners, a few respondents believed that the CMMC-AB RP badge helped them identify qualified consultants. Fortunately, only a small minority of respondents believed that the RP badge implies expertise.

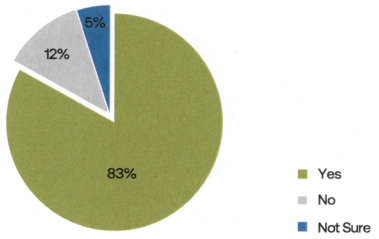
To steer industry to qualified professionals who can help with implementing the CMMC, the DoD and the CMMC-AB could leverage the DoD Cyber Workforce Framework (DCWF) to communicate to industry the knowledge, skills, and attributes of qualified internal cyber workers or external consultants. The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).[5] The DCWF has a hierarchical structure with seven broad categories (e.g., "securely provision" and "oversee and govern"), 33 specialty areas (e.g., "systems administration" and "data administration"), and 54 work roles (e.g., "system administrator" and "technical support specialist"). Each work role contains a definition as well as a representative list of tasks and knowledge, skills and abilities (KSAs) describing what is needed to execute key functions. There is also a Certified Information Systems Auditor (CISA) certification issued by the Information Systems Audit and Control Association (ISACA), which could be leveraged to connote IT auditing expertise and experience.

THE COST OF THE CMMC DFARS RULE IS VASTLY UNDERESTIMATED

In the DFARS interim rule, the DoD claims that only 30% of the DIB would be expected to attain a CMMC ML3, while the majority (60%) will only need a CMMC ML1. This rule implies that only 30% of the DIB handles or needs to handle CUI, as CMMC ML3 or higher is required to handle CUI. But according to the IPC survey results, 83% of respondents handle CUI and ITAR (International Traffic in Arms Regulations) data (see Figure 4). While the IPC survey respondents may not accurately represent the actual distribution of companies in the DIB who handle CUI, the survey results indicate that DoD's assumption that a minority of the DIB handle CUI may be uninformed.

[5] U.S. Dept. of Defense Chief Information Officer, "The DoD Cyber Workforce Framework." (DCWF), https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx.

Figure 4: Does Your Company Handle Control Unclassified Information or ITAR Data?



Source: IPC Industry Survey, 2021.

The DoD estimates a CMMC ML1 will cost $2,999 for small entities, for both the contractor support and the C3PAO assessment. The DoD estimates a CMMC ML3 will cost small entities $26,214 in nonrecurring engineering costs, $41,666 in annual recurring costs, and $51,096 for contractor support and the C3PAO assessment. Thus, the cost of a CMMC ML3 in the first year is more than $118,000. The cost difference between the CMMC ML1 and CMMC ML3 is more than $115,000 per small entity.

The DoD believes there are 163,391 small companies in the DIB. The DoD estimates the total cost to small entities in the first 10 years of the CMMC to be $3 billion, based on the assumption that 30 percent of the DIB will need a CMMC ML3 (see Table 1).

Table 1: DoD Cost Impact of CMMC ML3 for First 10 Years

Level 3	Quantity Unique Small Entities					
Year	Initial	Recert	Recert	Recert	Total	Total Cost
1	335	0	0	0	335	$39,856,827
2	1,661	0	0	0	1,661	$211,576,581
3	5,543	0	0	0	5,543	$742,647,086
4	10,624	335	0	0	10,959	$1,595,233,775
5	10,623	1,661	0	0	12,284	$2,105,527,148
6	10,623	5,543	0	0	16,166	$2,746,498,185
7	9,590	10,624	335	0	20,549	$3,342,948,078
8	0	10,623	1,661	0	12,284	$2,669,250,684
9	0	10,623	5,543	0	16,166	$2,867,603,803
10	0	9,590	10,624	335	20,549	$3,091,555,818

Source: U.S. Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)," Federal Register 85, no. 189 (September 29, 2020), pp. 61505-61522. https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf

If, however, one assumes that the distribution of the IPC survey results is representative of the CMMC ML3 distribution, the cost of the CMMC ML3 certification to small entities skyrockets from $3.3 billion in the 7th year of implementation (the most expensive year out of the first 10) to $9.3 billion. If the actual percentage of DIB companies needing a CMMC ML3 is between the DoD's estimate and the IPC survey results, at 60 percent, the cost in year seven is more than $6.6 billion to small businesses (see Table 2).

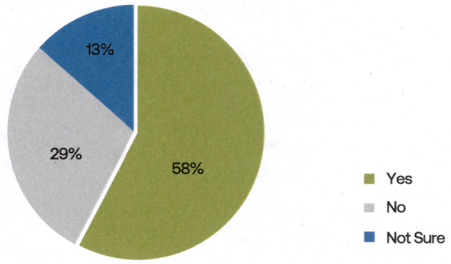
Table 2: Annual Costs of CMMC ML3, Three Scenarios

Year	Total Small Entities	Total Cost 30% ML3	Total Cost 60% ML3	Total Cost 84% ML3
1	335	$39,856,827	$79,713,654	$111,599,116
2	1,661	$211,576,581	$423,153,162	$592,414,427
3	5,543	$742,647,086	$1,485,294,172	$2,079,411,841
4	10,959	$1,595,233,775	$3,190,467,550	$4,466,654,570
5	12,284	$2,105,527,148	$4,211,054,296	$5,895,476,014
6	16,166	$2,746,498,185	$5,492,996,370	$7,690,194,918
7	20,549	$3,342,948,078	$6,685,896,156	$9,360,254,618
8	12,284	$2,669,250,684	$5,338,501,368	$7,473,901,915
9	16,166	$2,867,603,803	$5,735,207,606	$8,029,290,648
10	20,549	$3,091,555,818	$6,183,111,636	$8,656,356,290

Source: Author's analysis based on the DFARS CMMC interim rule and the IPC industry survey.

In addition to needing a CMMC ML3 at some point in the next five years, companies that handle CUI will also be required to conduct a NIST SP 800-171 self-assessment and submit their scores to SPRS as part of the DFARS-7019 Clause. While the self-assessment and reporting of the score is meant to be triggered by companies bidding on new contracts with the -7019 DFARS Clause, large prime contractors have been preemptively asking suppliers to conduct a self-assessment and to report their score into SPRS. At least 58% of the IPC survey respondents have already been asked by a prime contractor to conduct a NIST 800-171 self-assessment and to report the score to SPRS, before any solicitations with the -7019 Clause have been released (Figure 5). The respondents to the IPC survey overwhelmingly handle CUI and therefore the self-assessment requirements would apply to them at some point over the next three years. It is worrisome that more than half of the respondents have already been asked to conduct a self-assessment by a prime contractor, even though there is no legal or contractual requirement to conduct the assessment. According to DoD's cost impact analysis, "the need for a Basic Assessment will begin to impact entities as they compete on solicitations that include the new solicitation provision and contract clause, and the clause at DFARS 252.204-7012, if the entity has covered contractor information systems that are required to be in compliance with NIST SP 800-171."

Figure 5: Has Your Company Already Been Asked to Conduct a Self-Assessment?



Source: IPC Industry Survey, 2021

The NIST SP 800-171 self-assessment and reporting is estimated by DoD to take less than an hour and cost less than $100 per assessment. According to a NIST Cybersecurity Self-Assessment Handbok, "conducting security control assessments can be challenging and resource-intensive. Successful assessments require cooperation throughout the company. Establishing expectations before, during, and after an assessment is important to achieve an acceptable outcome. Thorough preparation is an important aspect of conducting effective security control assessments." The handbook also explains that, "It is expected that the business owner, chief operating officer, IT manager, security manager, and plant manager(s) will work together to assess the security of the system(s) that process, store, or transmit CUI."[6] Based on NIST's advice for preparing for and conducting a NIST 800-171 self-assessment, it would take much longer than an hour and cost more than $100 to conduct one properly. NIST does not provide an estimated number of personnel hours needed to properly conduct a NIST 800-171 self-assessment, but with 110 controls and more than 200 assessment objectives, it can be estimated that at least 30 minutes is needed to assess each control; properly acknowledging some controls will take far longer; and others much less. At 30 minutes per control, the NIST 800-171 self-assessment would take 55 hours to complete. Using a journeyman-level-2 rate of pay of $99/hour, a basic self-assessment would cost $5,445, which is $5,300 more than DoD's estimate of $73.30.

[6] U.S. National institute of Standards and Technology (NIST), "NIST MEP Cybersecurity Self- Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements," https://nvlpubs.nist.gov/nistpubs/hb/2017/nist.hb.162.pdf

In their impact analysis, DoD claims the annualized cost of the self-assessments is $971,083, based on a cost of $74.31 per self-assessment for 40,824 entities (and one assessment every three years). The self-assessment requirement, however, is going to impact far more than 40,824 companies because every company that handles CUI must conduct the self-assessment. According to the DFARS interim rule, at least 30% of the DIB will need a CMMC ML3, which implies that they handle CUI. The DoD estimates there are 220,000 companies in the DIB, which means that there are closer to 66,000 companies that will need to conduct a NIST 800-171 self-assessment. Currently, more than half (58%) of the IPC survey respondents are being required by prime contractors to conduct the self-assessment. If 58% of the rest of the DIB is being asked by a prime contractor for a self-assessment, the number of impacted companies jumps to 127,600 companies. If the price of the self-assessment is closer to $5,445 and the number of impacted companies is 30% of the DIB, as the DoD estimates in the interim rule, the actual annualized cost of the Basic self-assessment jumps from $971,803 to $119,790,000, which is 123 times more expensive than the DoD's total estimated cost impact to both the government and the DIB. If 58% of the DIB are required to conduct Basic self-assessments, the annualized cost jumps to $231,594,000, which is more than 200 times more expensive than DoD's total cost impact to the DIB and the government.

CONCLUSIONS AND RECOMMENDATIONS

President Biden's Executive Order on Improving the Nation's Cybersecurity instructs the Executive Branch to modernize FedRAMP (a cloud security framework), including identifying and mapping relevant compliance frameworks and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process. Likewise, the DoD can proactively modernize the CMMC along with the FedRAMP process by recognizing existing compliance frameworks.

The DoD and the CMMC-AB should establish qualification criteria for consultants so that the DIB is better suited to vet potential consultants for CMMC preparation. The DoD should help educate the DIB that the qualification criteria expressed as KSAs and a list of other attributes associated with qualifications (certifications, experience, and education) which demonstrate those KSAs. In the same way that DoDM 8570 establishes a list of baseline certification requirements for the DoD cybersecurity workforce, DoD should establish and publish baseline qualification standards for CMMC consultants and CMMC assessors that map to the DCWF.

To reduce the costs and burdens of the CMMC on the DIB, the DoD should consider leveraging existing industry standards and certifications. There are several widely adopted security standards and certification processes that have been implemented by thousands of companies around the world. The DoD should evaluate the level of risk mitigation and assurances provided by these existing certifications to determine if they provide equivalent or better protection for FCI and CUI. Recognizing additional

certifications currently available in the market will not only save DIB companies money and reduce the number of redundant audits by leveraging their existing certifications, but it will also create a pool of DIB companies who are able to bid on solicitations containing the CMMC DFARS clause. The CMMC-AB currently has no approved C3PAOs who may conduct CMMC assessments, but by recognizing other industry certifications, DoD will gain instant capacity for recognized assessments and a cadre of qualified and experienced assessors.

The U.S. electronics manufacturing industry is highly competitive with thin margins. DoD continues to assert that the CMMC costs will be recouped through general and administrative overhead costs in DoD contracts. This method of reimbursement favors late adopters and those that skimp on compliance expenses, which drives the industry to implement the bare minimum to pass the CMMC assessment. DoD should provide details into the method by which CMMC overhead costs are calculated and reimbursed. Overhead costs vary greatly from company to company, with no transparency to the DoD nor to the rest of the industry. The U.S. electronics manufacturing industry cannot remain in the DIB if they are forced to subsume additional overhead costs to remain competitive against peers who calculate their general and administrative CMMC costs differently.

About the Author

Leslie Weinstein is an Army Reserve Major with more than 15 years of experience consulting and working for the Department of Defense. In addition to her experience on active duty at the Defense Intelligence Agency and with offensive cyber operations at Army Cyber Command, Leslie has consulted for the Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD (A&S)), the DoD CIO, and the Air Force. As a consultant, Leslie focused on cyber policy and strategy and contributed to several initiatives impacting the entire DoD cyber workforce, including the DoD Cyber Workforce Framework and the Cyber Excepted Service. Leslie is currently serving as the Solutions Director for HITRUST.

Leslie has a Bachelor of Science degree in Management of Information Systems from the University of Alabama in Huntsville; a Master of Science in Strategic Intelligence from the National Intelligence University; and a Master of Business Administration from Cornell University.

IPC

BUILD ELECTRONICS BETTER

3000 Lakeside Drive, Suite 105 N
Bannockburn, IL 60015 USA
+1 847-615-7100 tel
+1 847-615-7105 fax
www.ipc.org

IPC is the global association that helps OEMs, EMS, PCB manufacturers, cable and wiring harness manufacturers and electronics industry suppliers build electronics better. IPC members strengthen their bottom line and build more reliable, high quality products through proven standards, certification, education and training, thought leadership, advocacy, innovative solutions and industry intelligence.

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

June 29, 2021

The Honorable Dean Phillips
Chairman, Subcommittee on
Oversight, Investigations, and Regulation
Committee on Small Business
United States House of Representatives
Washington DC, 20510

The Honorable Beth Van Duyne
Ranking Member, Subcommittee on
Oversight, Investigations, and Regulation
Committee on Small Business
United States House of Representatives
Washington DC, 20510

Dear Chairman Phillips and Ranking Member Van Duyne:

On behalf of the National Defense Industry Association (NDIA) and its Small Business Division leadership - thank you for holding the hearing: "CMMC Implementation: What It Means for Small Business." It is very encouraging to see members of the Small Business Subcommittee on Oversight, Investigations, and Regulation interested in Cybersecurity Maturity Model Certification (CMMC) program, its implementation, and the challenges it presents for small businesses within the Defense Industrial Base (DIB).

The process of implementing CMMC is a perfect example of the need for industry and the government to work together, to collaborate on the best path forward to shore-up our infrastructure, and do so in a way that is supportive and inclusive to the realities of small business participation in the DIB.

As an association, the National Defense Industrial Association (NDIA) represents nearly 1,600 corporate and over 70,000 individual members from small, medium, and large contractors; our members and their employees feel the profound impact of any policy change affecting how the United States equips and supports its warfighters. The immediate operational and financial implications of policy changes such as CMMC are especially challenging for our small business members as they attempt to recover from the COVID-19 pandemic.

NDIA is broadly supportive of securing the data and systems that drive the DIB, emphasizing implementability, affordability, and effectiveness. We are writing, for the record, on the challenges small businesses within the DIB face with CMMC implementation.

There are several complications we see regarding the path forward for CMMC implementation, including:

- **Cost:** Although the CMMC program office, and the regulatory language included in DFARS 2019-D041, has downplayed the cost to companies of compliance and repeatedly stated some compliance expenses will be allowed to pass on to the government, the actual costs companies like our members face to both attain compliance and receive certification are well above program office estimates. The extent of the allowability of these costs also remains uncertain and will potentially be limited to just a small part of the total cost of compliance.
- **Definition of Controlled Unclassified Information (CUI):** The lack of a 1) definitive, 2) specified, and 3) widely understood definition of CUI makes the current CMMC program un-

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

implementable and fraught with operational risk. As a contractor, it is difficult to make a determination during the course of performance about what information clearly is and is not CUI. While we are thankful to the Department of Defense (DoD) for recent guidance in this area, it still falls short of an operational definition that allows employees to easily identify, mark, and protect CUI. The DoD itself is also still struggling to adequately mark and identify information they pass to companies during the course of a contract as CUI. This issue is at the heart of CMMC level determination and has the potential to cripple the program if not adequately addressed. The complications exponentially increase when discussing the ambiguity and overlap between CUI, Covered Defense Information (CDI) and Federal Contractor Information (FCI).

- **Uncertainty with the CMMC Accreditation Body (CMMC-AB):** The history and continued uncertainty surrounding the CMMC-AB, the third-party nonprofit organization stood up by DoD, to include multiple resignations, allegations of conflicts of interest, changes in leadership, and shifts in mission have damaged the trust in the organization and increased complications relating to successful training and deployment of certified third-party assessment organizations (C3PAOs). We applaud the CMMC-AB for their recent efforts to train and move towards certifying C3PAOs, but it remains to be seen how quickly this body can scale its operations to meet the demands of the market and the goals set by DoD.
- **CMMC level classifications:** The classification of CMMC levels for contracts and subcontracts remains a critical concern with little transparency given to industry regarding the level-setting process and the impacts on developing the necessary contractor-subcontractor teams required to bid on and execute contracts successfully. The current plan for DoD acquisition professionals to determine the CMMC levels required by contracts and subcontracts creates an opportunity for variability across programs and drives complexity into the system. The possibility exists for companies to have contracts containing different CMMC level requirements for providing the same or similar products or services.
- **Long-term health of the DIB:** Last year, NDIA's Vital Signs the Health and Readiness of the Defense Industrial Base gave the health of the DIB a "C' grade. The costs and complexity of the current CMMC program constitute a burgeoning barrier-to-entry for new entrants and non-traditional companies to enter the defense market and may harm the long term health of the DIB. Today, with the current set of regulations and barriers in place, companies may have thought twice about entering into the defense industrial base. This barrier will rob the DIB, and ultimately our warfighters, of the competition, innovations, and new capabilities those companies could deliver.
- **Delineation of Information Technology (IT) systems and Operational Technology (OT) systems:** The current CMMC program does not delineate well between IT and OT leading to inappropriate blanket policies that complicate implementing the CMMC program in an OT-heavy environment, like those present in DIB manufacturing companies. Several companies within the NDIA Small Business Committee are very concerned about the content of the CMMC regulations and how they will impact their business. The CMMC controls fail to translate to a manufacturing and operational technology-rich environment, potentially alienating members of the DIB focused on manufacturing products for the DoD.

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

- Manufacturers help form the defense industrial base's backbone and ensuring their continued ability to compete and perform on government contracts should be a high priority. The operational technology "OT" utilized by manufacturers presents a unique challenge when trying to adopt the CMMC and NIST 800-171 standards. Special consideration should be given to developing guidance for both industry and government on how best to ensure that manufacturers are able to implement the cyber requirements and are not disadvantaged when audits are performed in an OT-heavy environment.

- **Duplicative Certifications:** The CMMC compliance regime, as currently contemplated, creates a system of duplicative certifications and requirements. This increases administrative complexity and costs for members of the DIB. For example, if a contractor achieves a CMMC Level of 3 or higher, would the contractor also be required to have a NIST SP 800-171 DoD Assessment under the DFARS 252.204-7019 requirements? If so, this would duplicate efforts because DoD has indicated that a CMMC Level 3 certificate demonstrates implementation of all NIST SP 800-171 security requirements. In order to avoid duplicative efforts for comparable assessments and provide clarity to contractors, subsequent policymaking should specify which assessments and levels are comparable and allow reciprocity between comparable assessments.

    - Some of our members have expressed that the CMMC practices and NIST 800-171 requirements do not contemplate the cloud-first world we increasingly live in, especially for small businesses. Therefore, subsequent policymaking should require DoD to accept GSA's Federal Risk and Authorization Management Program (FedRAMP) baselines as sufficient for CMMC compliance or expressly exempt cloud offerings from CMMC and allow FedRAMP to regulate cloud offerings. This allowance would be similar to DFARS 252.204-7012, which allows FedRAMP Moderate equivalent to meet some requirements for adequate security.

In the fall of 2020, NDIA submitted a list of outstanding questions to DoD and the CMMC-AB. We have yet to receive answers on a number of these questions, many vital to the successful execution of the program. *See attachment.*

While we continue to support the goal of the CMMC program to improve the cybersecurity of the DIB, we recognize there are serious challenges standing in the way of full implementation. We encourage this subcommittee to seriously consider requesting the DoD revise its policy to address the concerns we shared today. Supporting the importance of ensuring our defense industrial base remains the envy of the world and capable of providing our warfighters with the tools needed to succeed in any domain of conflict.

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

Thank you very much for your time and consideration. If we can provide further detail, or should you have any questions about these complications, please do not hesitate to contact us.

Sincerely,

Herbert J. Carlisle
General, USAF (Ret)
President and CEO

ML Mackey
Chair, Small Business Division, NDIA
CEO, Beacon Interactive Systems

ENLC: Outstanding Questions Sent to the DoD in 2020

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

Appendix: Outstanding Questions Sent to the DoD in 2020

October 7, 2020

Office of the Under Secretary of Defense for
Acquisition & Sustainment
Cybersecurity Maturity Model Certification

Office of the Under Secretary of Defense for
Acquisition & Sustainment
Defense Pricing & Contracting

Cybersecurity Maturity Model Certification
Accreditation Body

Re: Industry Questions on CMMC Implementation

To Whom It May Concern:

NDIA represents nearly 1,600 corporate and more than 70,000 individual members from small, medium, and large contractors dedicated to excellence in supplying and equipping America's warfighters. Policy changes have the potential to impact our members' effectiveness in supporting our military in their mission. As a result, our members are committed to active engagement with the Department of Defense by providing informed comment on relevant policies as they are developed and implemented. It is in this spirit that we provide the enclosed questions on the implementation of the Cybersecurity Maturity Model Certification (CMMC) program. This list of question builds on an initial set distributed to this community in late April 2020 of this year. Our questions draw broadly and deeply on the knowledge and expertise of leaders across the defense industrial base active in planning and preparing for CMMC compliance.

We appreciate DOD's prior engagement with industry to enrich and refine the model's specifications, and we look forward to continuing the dialogue as DOD fleshes out the administrative structures, processes, and procedures to manage implementation and compliance. As with our previous comments, these questions seek to clarify and optimize implementation of CMMC.

NDIA is fully supportive of the CMMC's underlying vision and plan to create a "unified cybersecurity standard for DOD acquisition." We urge DOD to continue providing industry with the opportunity to review and comment on DOD's proposed plans for the implementation and assessment of CMMC, preferably before any additional interim or final rules are promulgated to help inform and improve rulemaking

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

Questions (organized by theme):

I. General Administration
   a. Is the Department incorporating into the revision of the MOU between the AB and the CMMC office guardrails around the role of the AB to ensure that it remains a ministerial functionary that will ensure equity in the accreditation of C3PAOs and the issuance of certifications and not position itself as a gatekeeper controlling access to the federal market, creating pay to play mechanisms to let companies be certified or other undue control over the application of the standard on the DIB companies seeking certification? If so, what are those guardrails and, if not, why not?

II. CMMC Rollout
   a. How are the pilot/pathfinder contracts being identified? Will this information be made publicly available?
   b. What information will be made public following the conclusion of the pilot/pathfinder exercises?
   c. What programs are being prioritize for CMMC rollout?
      i. Simply including this information in the RFI/RFPs may not give a company sufficient time to respond, depending on the proposal timeline, CMMC level, and especially if you are a subcontractor under the program and may not see the RFI yourself – if DOD has key aerospace competitive programs in mind they want to target in 2021, it would be helpful to share that with industry. If they plan to target certain sole-source contracts, would also be helpful to know.
   d. Can the DOD update its FAQ online to address the most current questions about implementation from the Department's perspective?
   e. While DoD has readily made available its experts on CMMC to participate in countless industry outreach events both in person and virtually, it is not possible for members of industry to attend every event or follow every development. Will DoD commit to posting all CMMC industry events on its website as it did initially?
   f. CMMC: for 2020-2025, the interim rule says it applies if the contract has both the new -7021 clause AND the SOW lists a CMMC level. What if the RFP/contract only has the -7021 clause? DoD should give COs guidance not to include the clause (even if the rule goes into effect in 60 days) if there is no CMMC level in the SOW and it doesn't actually apply.

III. Costs
   a. What additional information is currently available about the allowability of costs associate with CMMC compliance and how they will be recovered? DOD has been clear that companies need to prepare for CMMC and that has resulted in companies incurring

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

costs associated with preparing for compliance – are they expected to be indirect costs or direct costs (for levels 4 and 5)?

b. In connection with the Regulatory Impact Analysis, has DOD included the costs that will be incurred by contractors in completing plans of action and milestones in order to achieve CMMC status?

IV. Assessments

a. Embrace need for annual Assessor visits. Technology isn't the answer for ensuring compliance. Certification (total audit) good for 3 years, intermediary years will require a Compliance Surveillance visit to cover part of controls and any areas of emphasis passed down by the CMMC CB (ISO standard approach and used on FedRAMP)
    i. Clears any ethical/company sensitive data access/security issues that surround using automated surveillance programs/software and the cost of such methods (standardization, verification, etc.).
    ii. Would eliminate the RFP under review
    iii. Follows successful ISO programs in use worldwide

b. Are assessments to be done on a CAGE code basis? If a contractor has multiple CAGE codes that share IT controls, will that be taken into account? Can a contractor schedule a single CMMC evaluation, for all its CAGE codes?

V. Assessments & Certifications

a. Is the C3PAO training process prepping audit companies to understand the nuances of every different IT and manufacturing Operational Technology (OT) environment?
    i. The DIB is full of technical complexity and nuance that may result in "false negatives" (failing a contractor) because the assessor lacks the technical competence and skills to understand what is likely to be many ways to approach some of the controls.
    ii. How will the DoD ensure consistency of the interpretation and application of requirements between C3PAOs and government auditors? How will the situation be handled if a C3PAO certifies a firm but a government auditor disagrees with the findings?

b. It seems that certification audits are likely to include the target company trying to "sell" their controls to the C3PAO as adequate and sufficient to meet the standard. Highly likely that companies will ask their outside cyber consultants to be present at the assessment to help "argue the cause." How is the CMMCAB approaching this? Will outside cyber advisors be allowed to be present?

c. How does the DOD and the CMMCAB plan to ensure consistency among the C3PAOs? Will there be an audit process to ensure C3PAOs are consistent and comprehensive in their assessments?

d. What oversight will there be over C3PAOs ability to set their own prices?

NDIA
2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

e. Given that the C3PAOs will be performing some traditionally governmental functions, what oversight will the DOD retain over these actors? To what extent would ethics rules applicable to Government employees be passed on to C3PAOs? For example, would any rules prevent or restrict an assessor from "switching sides" to go work for an organization seeking certification?
f. What systems and mechanisms have been developed to resolve disputes regarding C3PAO assessments and what recourse will contractors have? Are there plans for contractors to have recourse to DOD?
g. What considerations have been given to the recourse options available to subcontractors that fail C3PAO assessments? Will this cause delay on performance of the contract? Will a subcontractor seeking to remediate shortcomings be given expeditated processing for re-assessment?
h. Will C3PAOs be liable for any losses incurred due to a disputed assessment, where the C3PAO was found to be in error?

VI. CMMC-AB
a. While industry recognizes the hard work of the all-volunteer CMMCAB and their commitment to our shared mission, what legal and contractual protections are in place to prevent actual or potential conflicts of interest by Board members? Many CMMCAB members have business interests outside the AB and the DOD itself is bound by strict ethical rules. What rules will apply to the CMMCAB? Will these rules be included in the new Statement of Work agreement between the CMMCAB and the DOD?
b. Will the Statement of Work between the DOD and the CMMCAB be publicly released?
c. Has restructuring the CMMCAB to be more in-line with the ISO model been considered?
d. Has the CMCMAB considered a model where they hire and train assessors? This would allow the CMMCAB more quality control mechanisms over the C3PAOs and ensure consistency in audit performance and price.
e. If the CMMCAB does hire assessors, as the draft rule permits, how will they prevent conflicts of interest between their purported role as honest broker for the certification process and favoring their assessors in the certification process to drive business to the AB?

VII. Certification Levels
a. As many people have pointed out, there remains uncertainty about what criteria agencies will use to determine CMMC levels, how the agencies will ensure consistency in such determinations, and who will be responsible for determining CMMC levels for lower tiers? When can industry expect to see guidance on this issue to help plan for upcoming CMMC pilots?

NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

VIII. CUI

a. Can the DoD provide an update on progress of the CUI Handbook?
b. What training and materials will be made available to contractors for the handling of CUI? Online courses? DAU materials?
c. What controls will be in place to ensure the Services are compliant with the CUI marking standards prescribed in DODI 5200.48?
d. DoD has inconsistently used the phrases "CUI" and "DoD CUI" – are they intended to be used interchangeably? Is it intended to be the same universe as today's CDI? Put differently, is there any gap between the universe of CDI today and the CUI covered by the rule?

IX. DFARS Rule

a. To what extent will there be reciprocity between the DCMA cybersecurity assessments that have been conducted to date and future cybersecurity assessments under the DFARS interim rule?
b. Will the Interim Final Rule go into effect immediately upon issuance, thereby enabling the Services to invoke the CMMC in new contracts, Mods, SOW change orders; or will it be restricted to only new contracts in accordance with the CMMC phased roll-out?
c. The Interim Rule says COs have to verify, "for contractors that are required to implement 800-171", that contractors have an active assessment before they can award contract extensions – will the requirement to have an assessment will apply to existing contracts who have an option exercised after the effective date?
d. The Interim Rule says COs have to verify, "for contractors that are required to implement 800-171", that the contractor has a current assessment. Does that mean only contractors who actually receive CUI (and trigger the clause) have to submit? Or any contract that contains the -7012 clause will be required to submit? Many contracts may contain the -7012 clause but no CUI is exchanged or generated, and it would be helpful to provide guidance to contracting officers about this distinction.
e. How will DoD decide when to do a medium or high assessment?

NDIA stands ready to discuss our questions in-depth should you so desire. As our previous engagement on this issue shows, we would be happy to participate in dialogue on the CMMC program, its requirements, and its implementation, to ensure that the program achieves its objectives in a manner that respects the needs and concerns of its stakeholders.

If you or your staff have any questions, please contact Wes Hallman, Senior Vice President, Policy and Strategy, at whallman@ndia.org or (703) 522-1820.

Respectfully Submitted,

National Defense Industrial Association