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:

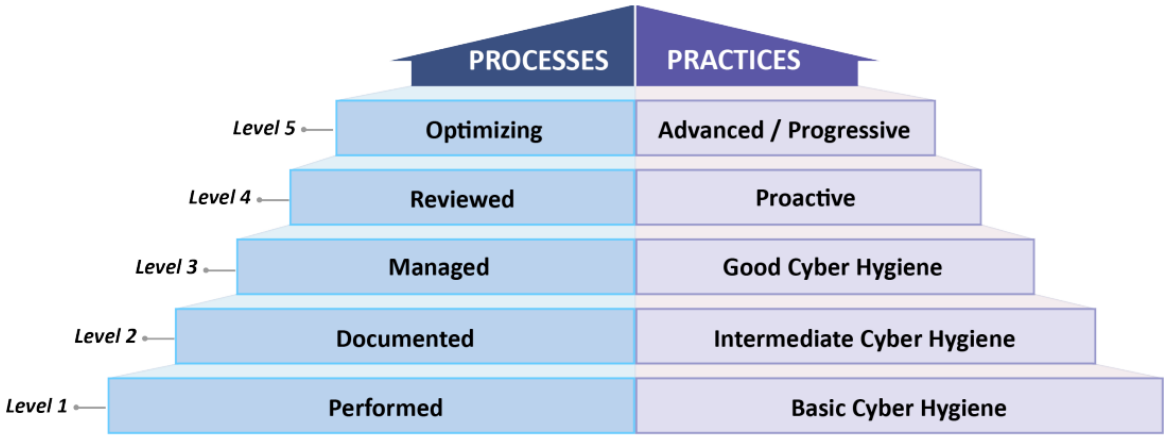

Figure 2. CMMC Levels and Descriptions

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.