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).