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-

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.

- 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.

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

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

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

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?

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?

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