2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

October 8, 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 more than 1,700 corporate and over 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

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.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 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

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

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?

2101 WILSON BOULEVARD, SUITE 700
ARLINGTON, VA 22201-3060
(703) 522-1820 • (703) 522-1885 FAX
WWW.NDIA.ORG

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