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

April 22, 2020

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

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, pursuant to an action item from the 6 March 2020 Tri-Association meeting. 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.

These questions follow earlier NDIA comments submitted to DOD pertaining to early versions of the CMMC Model. 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.

Questions (organized by theme):

I. COVID-19
   1. Given the current global economic crisis associated with COVID-19, is DoD or OMB re-evaluating the potential cost impact of the CMMC program on the supply chain? For example, is DoD considering delaying implementation of CMMC so that companies, particularly small to mid-sized companies, will have some time to recover before implementing controls above Level 1?

II. Certification Requirements, Processes, and Procedures
   1. Can companies hire subcontractors to do the assessments, and, if so, will the training and certification requirements be the same as for the company on contract to do the assessments?
   2. A DoD representative has hinted that certifications will be good for three years after receiving it. Is that going to become policy? Will a federal organization, like DCMA,

perform audits sometime in that three-years to ensure they are still adhering to the standards of the attained maturity level? If not, why not?

3. Does DoD plan to certify individual programs or systems for CMMC at Levels 4 and 5? If so, will those programs or systems inherit the corporate-level controls and capabilities, or will there be a need to replicate such controls and capabilities in a segregated area plus a need to achieve additional practices to get to higher certification levels?
4. If a subcontractor has only a small amount of CUI (e.g., an export controlled document) that relates to a lower risk component, will it be possible for a risk determination to be made to adjust the required level below Level 3 or will all companies with any type or amount of CUI be required to be at Level 3?
5. Is DoD open to a flexible scoring system for Levels 4 and 5 so that not all practices need to be met in a particular operational area if a contractor's maturity is greater in another area to offset the risk?
6. Will certified contractors run the risk of de-certification during the course of contract performance? Will there be periodic audits to determine if a contractor remains at a certification level? What about certification at the lower tiers of the supply chain?
7. Will certification levels of individual companies be public? How will companies know what CMMC level other companies (including their subcontractors) have achieved?
8. We are concerned that generally the contracting officer, program manager or representative will lack a calibrated way to determine the right CMMC level for an RFP and thus, to avoid any chance of criticism, they will simply designate it as Level 3 or higher by default. How can the government representative be confident and show justification in assigning a CMMC level lower than Level 3 whenever that is appropriate?

III. Compliance Costs

1. How exactly will recovery of the costs associated with becoming certified at the appropriate CMMC level work? Is recovery limited to incremental costs incurred necessary to meet the CMMC certification? If so, does that mean, for example, that only those costs to meet the 20 controls for CMMC Level 3 over and above NIST 800-171 are eligible?
2. If a company is newly entering the defense industrial base, would costs to align with NIST 800-171 and then to become CMMC Level 3-certified become costs eligible for recovery?
3. Will only contract "winners" be eligible, or can "losers" also seek reimbursement?
4. Does reimbursement only work for primes and their large bid packages, or for all DoD procurements?
5. Do primes' recovery allow them to "fund" the certification of their subcontractors' CMMC-related costs?
6. Will any CMMC costs be directly chargeable to programs and under what circumstances?
7. Will there be one established rate for assessors to conduct to a business? The assessor is certifying in the interest of the government. In most cases, if the government wants a third-party assessor (i.e., SMOG Check, VA Vehicle Inspection) the rate it the same no matter where or whom you go to.

8. Will the DoD or the CMMC-AB put out a cost estimate of what it will take for a company to be certified at each level?

IV. Supply Chain Flowdown

1. How, when, and by whom will CMMC levels be determined for a multi-tiered supply chain working on separate, discrete aspects of a program? For example, will the Government determine in the RFP which CMMC levels apply to the prime contractor's supply chain? Will the prime/higher-tier contractor have an opportunity to obtain DoD approval to flow down to a lower-tier subcontractor a lower CMMC level than the CMMC level identified for the prime contract? Or will the contractor have discretion to determine the CMMC level for the next tier below? Will the subcontractor have any responsibilities for notifying the prime contractor of issues with the CMMC levels and be required to flow down to lower levels?
2. In the early implementation of CMMC, if there are no suppliers for particular parts, equipment or services that have received assessments at the appropriate level, will prime contractors be able to apply for waivers so that they can successfully deliver products and services to the Government?
3. If a subcontractor or supplier does not have access to Federal Contract Information (FCI), but the subcontractor or supplier receives DoD funding, will the subcontractor or supplier be required to obtain a Level 1 certification?
4. Will all prime contractors, subcontractors, and suppliers that receive DoD funding be required to obtain at least a Level 1 certification, or is the level of certification dependent on the access of information? For example, does lack of access to Federal Contract Information (FCI) or critical program information obviate the need for Level 1 certification?
5. Will there be a grace period after contract award for subcontractor or suppliers to obtain CMMC certification?
6. Will there be CMMC exceptions for international suppliers? If yes, how will that work?
7. Will the contract specifically identify the level of certification for subcontractors and suppliers or will the contract delegate that authority to the prime contractor to determine the level of certification based on the subcontractor/supplier access to information?
8. What is the roll-out of all DoD contract assignments to a CMMC level over the 2021-2026 period, so companies have maximum advanced knowledge of the CMMC level for their products and services? Are certain procurement classifications to receive their CMMC level assignments in some known order?
9. What is the scope of the contractor's internal information that will be subject to third-party assessment and certification under CMMC? Will only those systems that house or process CDI or FCI be within the scope of the third-party assessment and certification?
10. Will DoD or certifiers advise contractors on the effect that a merger or a sale of assets will have on their certification level?

V. CMMC Program Management

1. How often will assessors have to recertify skills and certifications?
2. Will companies that hire IT experts to do assessments have to have certifications like ISO 9000 or CMMC level 2 (as is the case on some MAC/GWAC contacts today)?
3. If the CMMC AB is not yet funded and, once funded, has to secure office space, hire staff and initiate operations (and given the COVID 19-related slow-down), then is it likely that the pathfinder contracts scheduled for Fall 2020 will leak into 1Q21 if there is a material delay in standing up the AB.
    i. If so, how will this affect the next tranches of DoD contract ratings to CMMC levels?
    ii. Can the volunteer working groups really take up the slack, and will their work be accepted by the DoD and/or the AB?
4. Will assessors be required to have a degree in IT / computer science or at least some other IT training and certs like A+, Network+, Cloud+, and Security+?
5. Will DoD delegate authority to the individual Program Executive Offices (PEOs) or Program Offices to determine the requirements for certification?
6. What measures will be in place to ensure the third-party assessors will not use contractor proprietary information to gain an unfair competitive advantage? What confidentiality measures will be in place generally?
7. Will Government program offices, contracting officials, or agency heads have the flexibility to issue short-term or enduring waivers for specific programs or systems?

VI. Disputes, Adjudication, and Penalties

1. How can a company "appeal" the result of its CMMC assessment?
2. Will contractors have the right to appeal certification decisions to DoD if disputes about certifications cannot be resolved to the contractor's satisfaction by the Accreditation Body?
3. Does DOD anticipate that companies will be able to challenge the CMMC assessments of competitors in bid protests if a company loses an award to a competitor that the company has grounds to believe was rated too high?
4. What happens to companies that are not assessed in a timely manner? Will they be eligible for new bids? Would they lose existing business? Will contract options not be exercised?
5. What options will be available if a company being reviewed feels the assessor lacks sufficient knowledge, training and certification to do a fair assessment?

VII. CMMC-related Training

1. If assessor training is done online, how do you ensure the person taking the training is the one actually doing the future certification reviews?
2. In order to assist all, will DoD be putting together a matrix that will assist contracting officers and the DIB on how to determine CMMC levels for a RFP?
3. What training will be offered so that the assessors that have to work as a team to review offices/networks in multiple CONUS / OCONUS locations ensure there is a seamless review and nothing is missed?
4. When will DoD be training the acquisition community on CMMC? How will the training be conducted?

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

VIII. Interagency Issues

1. Companies have experienced conflicting opinions between DCSA auditors onsite when evaluating current compliance with the NIST 800-171. Will DCSA participate in the development of the CMMC certification criteria for operational technology?
2. What is the process to resolve CMMC interpretation discrepancies with government or third-party auditors?
3. Will DoD provide, in the proposed rulemaking, for reciprocity with the DCMA Strategic Assessments of DFARS implementation that already have been conducted so that contractors will not be required to re-establish implementation of the 110 controls that have been reviewed by DCMA?
4. Will DoD also provide for reciprocity for ISO, FedRAMP, and other certifications?

IX. CMMC Model Controls

1. There has been an increasing use of teleworking in the government contracting and larger commercial community, yet the CMMC v1.0 draft does not address how to handle the situation in which employees use their own devices to access and perform. We recommend that CMMC address this important development as it affects both the federal and contractor/supply chain workforces and is a potential security gap as those terminals presumably would be considered "endpoints."
2. What is the process with which the DoD and NARA will determine a stable definition of CUI as it relates to CMMC?
3. With respect to Levels 4 and 5, will all of the listed controls apply or will a subset be specified in the RFP? Will companies be permitted more time to apply these more complex controls (i.e., will all controls need to be implemented by the time of award)?

X. Small Business

1. Small businesses need more clarity from DoD on what percentage of the contracts will require CMMC Level 1. Doing the math, the cost of obtaining Level 1 is significantly lower than CMMC Level 3. DoD representatives have been putting out contradicting information on what they expect.
2. When will the training come out for small businesses that can't afford to hire a dedicated or part-time IT consultant to set up a certifiable network, and how many hours will it take to educate companies so they understand basic security measures such as firewalls, switches, routers, DMZ's, MFA, token based encryption. What about advanced but relevant measures like closing off ports, monitoring open ports for potential intrusions, implementing DISA Security Technical Implementation Guides (STIGs), or doing basic JavaScript Object Notation (JSON) to set up the Amazon Web Services security for basic cloud file storage for FOUO/CUI?

XI. Manufacturing and Operational Technology

1. Some IT controls in CMMC v 1.0 are not suitable for operational technology (OT) systems, such as manufacturing systems. For example, safety may be adversely affected by requirements for multi-factor authentication or auto-logoff time limits. Factory floors often use old operating systems which cannot be patched and cannot run anti-virus

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

software. How will a supplier's certification be affected if OT systems are not in compliance with required IT controls?

2. How will the controls be implemented in manufacturing or other environments where some controls cannot be implemented without impacting the work being performed? Will there be an exemption for these environments? If not, will there be an exception process?
3. Manufacturers are in need of a cybersecurity solution that proactively protects an OT environment without requiring costly changes to manufacturing equipment. Such a solution would help accelerate full CMMC compliance by reducing cost and effort. That solution also could better enable secure trading partner connectivity – a key element needed for the defense industrial base to benefit from Industry 4.0. Could DoD mount a grand challenge to address this issue?

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