U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF ADVOCACY
REGULATION • RESEARCH • OUTREACH

September 25, 2019

VIA ELECTRONIC SUBMISSION

Ms. Katie Arrington
Chief Information Security Officer
Office of the Assistant Secretary for Defense for Acquisition
osd.pentagon.ousd-a-s.mbx.cmmc@mail.mil

Re: Department of Defense Draft Cyber Certification Model

Dear Ms. Arrington:

The U.S. Small Business Administration's Office of Advocacy (Advocacy) submits the following comments in response to the draft Department of Defense (DOD) Cybersecurity Maturity Certification Model (CMMC).

The Office of Advocacy

Congress established Advocacy under Pub. L. 94-305 to represent the views of small entities before federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA); as such the views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration. The Regulatory Flexibility Act (RFA),[1] as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA),[2] gives small entities a voice in the rulemaking process. For all rules that are expected to have a significant economic impact on a substantial number of small entities, federal agencies are required by the RFA to assess the impact of the proposed rule on small entities and to consider less burdensome alternatives.

The Small Business Jobs Act of 2010 requires agencies to give every appropriate consideration to comments provided by Advocacy.[3]

Background

DOD is seeking comments on a draft cybersecurity model. If implemented this model would impose a mandatory compliance requirement on every DOD supplier and contractor. The model consists of five levels of certifications. Contracts will not be awarded to a company without its

[1] 5 U.S.C. §601 et seq.
[2] Pub. L. 104-121, Title II, 110 Stat. 857 (1996) (codified in various sections of 5 U.S.C. §601 et seq.).
[3] Small Business Jobs Act of 2010 (PL. 111-240) §1601.

being certified in one of the five levels. It is estimated that more than 300,000 companies would have to comply with this proposed model

Advocacy's comments on the draft model

Currently DOD recognizes that the implementation of this model may require the agency to permit contractors to charge parts of their cyber development as allowable costs. Many DOD small prime and subcontractors operate on firm fixed priced contracts. This model is not clear as to how such businesses will be reimbursed or compensated for implementing the cyber compliance model.

The CMMC is a very complex and detailed program. This may dissuade small businesses from attempting to gain certification even when the requirements themselves are not deemed to be unduly onerous by the applicant. The low levels of maturity indicated by the Level 1 practices, however, raise the possibility that businesses certified at that level would not be considered suitable for many or most contracts. Put another way, the situation that Advocacy is keen to avoid involves defining levels which are attractive to small businesses and levels which are actually sufficient for contracting, with no overlap between the two. This factor may have a tremendous negative impact on DOD achieving its statutory annual procurement goals for small businesses.

Advocacy is concerned with the significant gap in capability between the lower and higher levels of certification which may create a low-certification trap in which low levels of certification are obtainable by small businesses, but the majority of contracts require higher levels of certification. One method possible for both reducing overall complexity of the program and ensuring that a low-certification trap is not inadvertently created is to employ a cost-benefit analysis to the progression across levels within each domain to ensure that each step presents the most cost-efficient increase in security available. For example, Level 3 of the Identification and Domain Authorization domain includes several password novelty and complexity requirements, while Level 4 introduces multi-factor authentication. But, as Alex Weinert of Microsoft recently argued, "it may well be that traditional password concerns no longer have much effect on actual security, while the effect of multi-factor authentication may be much higher."[4] Thus, while password controls are relatively simpler to implement, multi-factor authentication could have a larger impact dollar for dollar and hour for hour. This example is merely illustrative of the approach that might be taken, and other factors may rightly govern decisions made about these particular requirements.

Advocacy believes that small businesses may have problems with the complexity of the program. It features 18 domains, for which there are five levels assessed along multiple practices and processes for each level. The draft notes the addition of 230 practices across the five levels since the previous revision of the document. This multi-layered approach creates a combinatorial explosion of cognitive costs which affects small businesses. The CMMC brief notes that "Down-selection, prioritization, and consolidation is still to occur." Advocacy hopes

[4] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identify/Your-Pa-word-doesn-t-matter/ba-p/731984.

that when these activities do take place, they are used to aggressively pare down the number of individual considerations to the minimum practical.

Lastly, the briefing document notes that "[the] goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels." Advocacy applauds this specific consideration for small businesses. Advocacy has previously submitted a comment letter on a DOD cyber rule and is gratified to see that some of the comments have been taken into consideration in the development of this model. Please refer to our previous comment letter.[5]

Conclusions and Recommendations

Advocacy believes that this, and any other model, should be subjected to public review. It is unclear from the proposal how many small businesses and small business experts participated in the development of this model. It is Advocacy's recommendation that because of the extensive cost compliance and the impact of this model on small businesses it should be subjected to the notice and comment rule making process.

Advocacy urges DOD to give full consideration to the above issues and recommendations. We look forward to working with you as we explore these new opportunities and challenges facing the federal government in cybersecurity.

If you have any questions, or require additional information, please contact me at 202-205-7150 or major.clark@sba.gov.

Sincerely,

/s/

Major L. Clark, III
Acting Chief Counsel
Office of Advocacy
U.S. Small Business Administration

Copy to: The Honorable Howard Shelanski
Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget

[5] https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/24161055/DFARS_security_interim_comment_letter.pdf