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

February 26, 2024

VIA ELECTRONIC SUBMISSION

John Sherman
Chief Information Officer
U.S. Department of Defense

Re: Cybersecurity Maturity Model Certification (CMMC) Program (DoD-2023-OS-0063)

Dear Mr. John Sherman,

On December 26, 2023, the Department of Defense (DoD) published a proposed rule entitled Cybersecurity Maturity Model Certification (CMMC) Program.[1] This proposed rule intends to create a mechanism by which the DoD can certify contractors and subcontractors are in compliance with cybersecurity guidelines. This letter constitutes the Office of Advocacy's (Advocacy) public comments on the proposed rule.

Advocacy is principally concerned with the ability for small businesses to meet and comply with the standards and timelines set out in the CMMC Program without further clarification and guidance documents from the DoD. The current rule does not provide clear guidance on the process to create enclaves, which would allow more small business subcontractors to participate in DoD contracts without meeting the full requirements necessary for the prime contractor. Advocacy seeks clarification on the role of Third-Party Assessment Organizations (C3PAO) and the indemnification a C3PAO has if a contractor or subcontractor is out of compliance. Additional concerns include the process of how and if more C3PAOs can be certified by the DoD to review the numerous contracts that will be subject to certifications. Advocacy urges the DoD to provide clarification about the enforcement mechanisms for breaches of cybersecurity. Lastly, Advocacy reminds the DoD that this rule will impose a high cost of compliance on small businesses and any means to reduce the burden on small businesses will increase the participation of these impacted businesses.

[1] Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. 89058 (Dec. 26, 2023) [hereinafter Proposed Rule].

I. Background

A. The Office of Advocacy

Congress established the Office of 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) that seeks to ensure small business concerns are heard in the federal regulatory process. Advocacy also works to ensure that regulations do not unduly inhibit the ability of small entities to compete, innovate, or comply with federal laws. The views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration.

The Regulatory Flexibility Act (RFA),[2] as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA),[3] 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, the RFA requires federal agencies to assess the impact of the proposed rule on small entities and to consider less burdensome alternatives.[4] If a rule will not have a significant economic impact on a substantial number of small entities, agencies may certify the rule.[5] The agency must provide a statement of factual basis that adequately supports its certification.[6]

The Small Business Jobs Act of 2010 requires agencies to give every appropriate consideration to comments provided by Advocacy.[7] The agency must include a response to these written comments in any explanation or discussion accompanying the final rule's publication in the Federal Register, unless the agency certifies that the public interest is not served by doing so.[8]

Advocacy's comments are consistent with Congressional intent underlying the RFA, that "[w]hen adopting regulations to protect the health, safety, and economic welfare of the nation, federal agencies should seek to achieve statutory goals as effectively and efficiently as possible without imposing unnecessary burdens on the public."[9]

B. The Proposed Rule

The proposed rule would give contractual effect to NIST SP 800-171 and 172, requiring companies to meet the three levels of compliance if the contracts involve FCI or CUI. CMMC attempts to redesign previous iterations of cybersecurity models with a more streamlined process. This proposal would simplify previous systems to create a more streamlined certification system. This rule differs from previous iterations by allowing for businesses to create enclaves within their business models, allowing the business to implement the CMMC standards while not drastically changing every aspect of their business process.

---

[2] Pub. L. No. 96-354, 94 Stat. 1164 (1980) (codified at 5 U.S.C. §§ 601-612).
[3] Pub. L. No. 104-121, tit. II, 110 Stat. 857 (1996) (codified in scattered sections of 5 U.S.C. §§601-612).
[4] 5 U.S.C. § 603.
[5] *Id.* § 605(b).
[6] *Id.*
[7] Small Business Jobs Act of 2010, Pub. L. No. 111-240, §1601, 214 Stat. 2551 (codified at 5 U.S.C. § 604).
[8] *Id.*
[9] Regulatory Flexibility Act, Pub. L. No. 96-354, 94 Stat. 1164 (1980) (codified at 5 U.S.C. §§ 601-612).

Under the proposed rule, the CMMC Program will require all DoD contractors and subcontractors who handle federal contract information (FCI)[10] and Controlled Unclassified Information (CUI)[11] to maintain cybersecurity protections of their systems.[12] CMMC will create three levels of compliance, depending on the level of security necessary for which the contractor has access. Level 1 has 15 requirements focused on logging access to potential FCI.[13] Level 2 includes minimum requirements for contractors handling CUI and adds 110 requirements.[14] Level 3 addresses an additional 24 requirements.[15] Each level will pose varying challenges for small businesses of every kind to comply with the progressing requirements. Advocacy has commented on previous proposals for CMMC concerning the significant impact this will have on small business contractors.[16]

II. Advocacy's Small Business Concerns

Advocacy held outreach meetings with diverse small business stakeholders concerning this rule, both in-person and virtually. Small businesses expressed concerns with how to compensate the increased costs due to implementing CMMC and asked for clarity on aspects of the proposed CMMC rule. Advocacy has four chief concerns with the proposed rule.

A. Advocacy requests clear and concise guidance for small business contractors and subcontractors to create enclaves in order to lessen the burden of compliance on the businesses.

The proposed rule states that different business segments or different enclaves of a business can be assessed or certified at different CMMC levels.[17] Creating and implementing enclaves will be most effective when a large prime contractor creates these enclaves to ease the burden on small subcontractors. The rule mentions the use of enclaves but does not provide guidance on *how* to implement enclaves within a business.

External service providers (ESPs) will be a driving force for small businesses' compliance with CMMC. ESPs are vendors that handle security related data or CUI on their own assets and software. The ability of ESPs to create effective and economically feasible software will allow businesses to enclave different operations more easily and avoid unduly costly compliance expenses.

Advocacy recommends that the DoD create a presumption to reduce the number of small contracts that are subject to CMMC Level 2. This can be achieved through varying means, including a positive requirement for prime contractors or the ability for a prime contractor to

[10] Defined in FAR 52.204-21.
[11] Defined under DFARS 7012.
[12] Defined in FAR 52.204-21 for FCI and NIST SP 800-171 and 172 for CUI.
[13] Proposed Rule, *supra* note 1, at 89,065.
[14] *Id.*
[15] *Id.*
[16] U.S. Small Bus. Admin., Off. Of Advocacy, Comment Letter on Proposed Rule for DoD CMMC (Sep 25, 2019), https://advocacy.sba.gov/wp-content/uploads/2019/09/comment-letter.pdf.
[17] *Id.* at 89,071.

engage in using enclaves as a positive value marker for their contracts. Further, the agency contracting officer could be required to engage in mitigating efforts if such CMMC related issues arise between a subcontractor and prime contractor.

B. Advocacy seeks clarity on the role of C3PAOs and the ability of C3PAOs to meet the demand for CMMC.

For CMMC Level 2 compliance, a third-party certifier (C3PAO) will triennially inspect the businesses' compliance with the 110 requirements of CMMC Level 2.[18] Stakeholders raised concerns regarding the role C3PAOs will play in Level 2 certification and sought clarity on the indemnification of issues arising from a certification. Stakeholders raised concerns that if there are an insufficient number of C3PAOs to timely inspect every contractor before the rule is effective, then small businesses will be the last ones to be certified. Advocacy recommends creating a streamlined process to provide organizations with C3PAO certifications. This process would meet the immediate need of contractors to initially certify with a C3PAO that the business meets CMMC Level 2 requirements. Particularly, there should be availability of C3PAOs for small businesses and ensure small business owners are not falling behind.

C. Advocacy asks the DoD to clarify enforcement guidelines/mechanisms.

As proposed, Level 1 contractors would annually attest their compliance with the requirements.[19] While at Level 2, there would be attestations with C3PAO certifications every three years.[20] Stakeholders raised questions about the practical steps the DoD will take in enforcement actions for breaches. Further, stakeholders raised concerns regarding the availability of remediating steps in the instance of failure to meet a CMMC requirement. Advocacy recommends the agency create guidance documents for small business contractors to better understand the legal effects of the CMMC.

D. Advocacy highlights the need for DoD to create rules that encourage and improve small business participation in contracting programs.

Advocacy reiterates the importance of small businesses in federal contracting.[21] Creating accessible, commercially viable, and secure cyber systems is critical for the future of national security. Small businesses wish to continue to be a powerful driver of national defense contracting.

---

[18] *Id.* at 89,065.
[19] *Id.*
[20] *Id.*at 89,060.
[21] *See* U.S. Dep't of Def., *DoD Releases Small Business Strategy* (Jan 26, 2023), https://www.defense.gov/News/Releases/Release/Article/3279279/dod-releases-small-business-strategy/ ("Small businesses make up 99.9 percent of all U.S. businesses as well as 73 percent of companies in the defense industrial base, and last year small businesses were awarded over 25 percent of all DoD prime contracts. As the economic engine of our nation, small businesses create jobs, generate innovation, and are essential, daily contributors to national security and the defense mission.").

Advocacy heard small business stakeholders from across the country express their strong commitment to protecting our country from cyber-attacks and recognize the critical need for CMMC and other cybersecurity measures.

Small businesses urge DoD to create flexibilities such as using Plan of Action and Milestones (POA&Ms) when this rule goes into effect initially, allowing small businesses to ramp up to full compliance with their respective CMMC level.

III. Conclusion

Advocacy's chief concerns surround a lack of clarity on key aspects of the proposed rule. Advocacy requests clarification from DoD as to how to create enclaves within businesses. Encouraging the use of ESPs and incentivizing large prime contractors to keep all subcontractors from being subject to high levels of cybersecurity will be key in keeping small businesses engaged in DoD contracting. Guidance documents for small businesses (especially aimed at the smallest of small businesses) and ESPs will create an easier ramp for small business compliance. Advocacy requests clarity from DoD regarding the role of C3PAOs and encourages the DoD to ensure small businesses can obtain certification from C3PAOs in a timely manner. Further, the DoD should clarify the enforcement and procedural repercussions for a failure to meet various CMMC levels. Lastly, the DoD should set achievable goals as CMMC is implemented, ensuring that current small businesses contracting with the agency can continue work with the government while ensuring our nation's defense.

If you have any questions or require additional information, please contact me or Assistant Chief Counsel David Mullis at (202) 830-2292 or by email at David.Mullis@sba.gov.

Sincerely,

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

David Mullis
Assistant Chief Counsel
Office of Advocacy
U.S. Small Business Administration

Copy to: The Honorable Richard L. Revesz, Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget