PSC PROFESSIONAL SERVICES COUNCIL

November 30, 2020

Mr. John M. Tenaglia
Principal Director, Defense Pricing and Contracting
Office of the Assistant Secretary of Defense for Acquisition & Sustainment
Department of Defense
3060 Defense Pentagon, Room 3B938
Washington, DC 20301-3060

Subject: Comments on Interim Final DFARS Rule: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

On behalf of the member companies of the Professional Services Council (PSC),[1] we are pleased to comment on the September 29, 2020 Department of Defense (DoD) Interim Final DFARS Rule: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041). This rule implements two related assessments of cybersecurity requirements: (1) National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800–171 DoD Assessment Methodology and (2) the Cybersecurity Maturity Model Certification ("CMMC") Framework. PSC supports DoD's efforts to create a unified cybersecurity standard based on "best practices" to secure the defense industrial base. However, PSC has some concerns, recommendations and questions regarding both the NIST SP 800–171 DoD Assessment Methodology and the CMMC Framework covered in the Interim Final DFARS rule, as detailed below.

NIST SP 800–171 DoD Assessment Methodology

The Interim Final Rule enforces what the DoD acquisition community has consistently asked of contractors and subcontractors in past contracts through DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. The Interim Final Rule requires a company to complete a basic assessment of their implementation of NIST SP 800–171 against a DoD-provided scorecard template and upload its score into the DoD-controlled Supplier Performance Risk

[1] PSC is the voice of the government technology and professional services industry, representing the full range and diversity of the government services sector. As a trusted industry leader on legislative and regulatory issues related to government acquisition, business and technology, PSC helps build consensus between government and industry. Our over 400 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the trade association's members employ hundreds of thousands of Americans in all 50 states.

System (SPRS). Self-scoring, especially by multiple levels in the supply chain, helps primes assess risk of their supply base and allows small businesses to determine what they need to do to meet cyber compliance. However, it is possible that many small businesses may fail to meet the SPRS self-scoring deadline. It is also likely that not all impacted small businesses are even aware of the requirement. **What happens if companies don't comply with this self-assessment requirement by the deadline? When would those consequences occur (e.g. on their next award/option/task order)?**

A basic self-assessment doesn't automatically result from a common application of the NIST 800–171 standards. Companies with the same capabilities and security practices may assess themselves differently by applying a different standard for compliance with the NIST SP 800–171 security requirements. Including self-assessment scores as part of source selection criteria, whether implicitly or explicitly, incentivizes companies to apply a less stringent standard in their self-scoring. This lack of comparability across the defense industrial base would not be a valid basis for DoD acquisition decision-making since there would be a significant potential for an inherent lack of consistency. **Why would the Department impose a rule that prohibits, or at least discourages, competitive analysis, evaluation, or source selection based on these self-assessments?**

Self-assessment scores could lead to increased False Claims Act (FCA) allegations as subcontractors may enhance their cyber hygiene scores in order to stay competitive or, if they do not meet the conditions of their Plan of Action & Milestones (POA&Ms), to correct deficiencies to obtain the perfect score of 110 by a certain date. Self-assessment scores could also lead to increased protests, reduced privacy for subcontractors, and general anti-competitiveness that may induce sole source selection down the supply chain. Additionally, this factor may decrease the number of subcontractors used if primes are communicating to other primes what scores their suppliers have –as subcontractors may work at different levels for different primes. **As a prime contractor's self-assessment scores are uploaded into the SPRS prior to contract, will the prime's supply chain also need to upload their own scores into the SPRS prior to the award to the prime?**

There are other concerns beyond the self-assessment. This Interim DFARS Rule is not clear on reciprocity regarding other federal security standards, such as whether FEDRAMP or other security standards meet the baseline requirements of the NIST 800–171 controls. There is also a lack of clarity regarding what constitutes, or determines, the benchmark for being identified for a basic, medium, or high assessment related to a NIST 800–171 self-score. Additionally, there are questions regarding the coverage of the flow-down requirements.

There are also questions regarding contract evaluations. While the Interim Final Rule makes clear that 110 is the perfect score to fulfil cybersecurity requirements prior to a contract award, it does not clearly state that a perfect score of 110 is <u>required</u> prior to a contract award – only that a contractor and/or subcontractor must have a self-assessment score on record in the SPRS. Any final rule should clarify the threshold score and the timing of the evaluation of the score that is uploaded into SPRS for a contractor or subcontractor to be awarded a contract. Any final rule should also clarify how

contracting officers will evaluate a company based on its score if there is no threshold prior to a contract award.

CMMC framework

On September 25, 2019, PSC sent a letter to DoD outlining concerns with the draft model and the broader CMMC program.[2] Those concerns included 1) clarity of definitions within CMMC, 2) adaptability of cybersecurity and innovation, 3) alignment with other audits, assessments and reviews, 4) consistency of implementation in source selection, 5) impact on competition, 6) certification flow-down, 7) third party certification, and 8) CMMC governance, training, and accreditation. We appreciate that most, but not all, of our concerns with respect to the CMMC model were addressed in subsequent clarifications. However, many questions remain even with these, as well as other aspects of the CMMC framework.

For example, there is still question regarding the adaptability of cybersecurity and innovation within the CMMC framework. It remains unclear how potential innovations would be incorporated into future revisions of the CMMC. For CMMC to be an effective tool for securing the industrial base, it will need to be updated in a timely fashion to reflect new technologies made available in the marketplace as well as changes to the "threat" and the methods used by our adversaries against our networks. Another area where PSC remains concerned is in the resourcing of CMMC governance, training, and accreditation. Furthermore, the relationship between DoD and the CMMC Accreditation Body lacks the transparency needed by all stakeholders to have a full appreciation of the program mechanics.

Conclusion

This Interim Final Rule lacks the clarity to address the issues described above regarding the NIST SP 800–171 DoD Assessment Methodology. In addition, there are substantial elements of the CMMC Framework that will create implementation problems but that cannot be addressed by simply making changes in a subsequent rule. Additional policy, process and structural changes are needed, including with regard to the Accreditation Body, assessor capacity, and threat changes.

PSC applauds DoD's engagement with the contractor community throughout the development of the CMMC, and we will continue to support efforts to secure the defense industrial base. However, given the structural concerns we addressed regarding CMMC and the NIST self-assessments as described above, this is not an exhaustive summary of all of our concerns or potential recommendations regarding the CMMC program.

---

[2] PSC feedback on DoD CMMC. "Re: DoD Request for Feedback of Draft CMMC Model Rev 0.4" September 25, 2019. https://www.pscouncil.org/psc/a/Resources/2019/PSC_Feedback_of_Draft_CMMC.aspx

Thank you for your attention to these comments. If you have any questions or need additional information, please do not hesitate to let me know. I can be reached at (703) 875-8059 or at chvotkin@pscouncil.org.

Sincerely,

Alan Chvotkin, Esq.

Executive Vice President and Counsel