WIN-TECH INC

Win-Tech, Inc.
8520 Cobb Center Dr.
Kennesaw, GA 03152

October 15, 2024

Re: Submission of Feedback/Public Comment, re: Assessing Contractor Implementaton of Cybersecurity Requirements (DFARS Case 2019-D041) 48 CFR Parts 204, 212, 217, 252 (Docket DARS-2020-0034) (RIN 0750-AK81)

As a small business manufacturer, I respectfully submit Win-Tech's comments to the Proposed Rule:

1. *"Require the contractor to include the requirements of the clause in subcontracts or other contractual instruments. The purpose of the clause is to ensure suppliers at all tiers are in compliance with the security requirements identified at 32 CFR part 170 when there is a requirement for CMMC in the contract, if applicable based on the information that is being flowed down."*

   Comment:

   Sub-contractors regularly fall victim to poor (or lack of) CUI markings, which lead to a mismatch of contractual flow down and actual properly-identified information that is transmitted.

2. In the same vein as the topic above:

   "Consult 32 CFR part 170 related to flowing down information in order to establish the correct CMMC level requirements for subcontracts and other contractual instruments;"

   32 CFR 170.23 states "*If a subcontractor will process, store, or transmit CUI in performance of the subcontract*" as its criteria.

   Comment and Recommendation:

   We agree with a peer's comment submitted on FR Doc # 2024-18110 in September 2024:

   As it stands this creates a perverse incentive for primes and higher tier subs to exercise this flow down in all solicitations, rather than applying discretion as to whether flow of CUI is actually [marked and shared].

   I would like to recommend that the final 48 CFR rule contain regulatory pressure on the contractor to justify flow downs as being critical to the execution of the program [based on marked and transmitted CUI].

Such regulatory pressure could keep many small businesses who do not actually store, process, and transmit CUI from leaving the DIB. Such regulatory pressure would conversely be a relatively small burden on primes and higher tier subs.

I whole-heartedly agree with this perspective and recommendation, per edits above.

3. *"DoD does not expect this proposed rule, when finalized, to have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, et seq."*

Comment and Recommendation:

The Regulatory Flexibility Act (RFA)'s goal is to ensure that federal regulations are not overly burdensome for small entities and to promote the small entities' abilities to compete with larger organizations.

In 48 CFR Parts 202, 204, 212, 239, and 252 (updated per 81 FR 72990, October 2016), DoD implemented the requirement that "*contractors shall implement NIST SP 800-171 as soon as practical, but not later than December 31, 2017*." Public comments related to costs for implementation were published with that Final Rule, along with DoD's responses. Comments in this Final Rule included concerns about cost and suggested the requirements were poised to push out small business. DoD replied: *"The cost of compliance with the requirements of this rule is unknown as the cost is determined based on the make-up of the information system and the current state of security already in place. If a contractor is already in compliance with the 2013 version of the clause 252.204-7012, then the changes necessary to comply with the new rule are not as significant."* Taking another step backwards and reviewing 48 CFR Parts 204, 212, and 252 Final Rule (updated per 78 FR 69273, November 2013) ("Requirements Relating to Supply Chain Risk"), comments complained about cost. DoD reassured stakeholders with:

"...it is estimated that 6,555 contractors would be handling unclassified controlled technical information and therefore affected by this rule. Of the 6,555 contractors it is estimated that less than half of them are small entities. For the affected small entities a reasonable rule of thumb is that information technology security costs are approximately 0.5% of total revenues. Because there are economies of scale when it comes to information security, larger businesses generally pay only a fraction of that amount."

DoD is mistaken to assume that this rule will only affect 6,555 contractors and that NIST SP 800-171-compliant contractors only spend 0.5% of their total revenue on compliance efforts.

This Proposed Rule suggests that at the end of the 4-year roll-out, nearly 30,000 companies (20,395 of those small businesses) must be Level 1 or Level 2 certified. The DIB has constrained, not grown, so assuming these recent numbers are accurate, the premise of all cost expectations from the 78 FR 69273 from November 2013 set the stage for erroneous calculations later.

I understand that this rule covers the incorporation of contractual requirements (rather than the CMMC program itself), but the 32 CFR 170 and the 48 CFR Parts 204, 212, 217, 252 are interwoven – they are both needed to be applicable to industry. The CMMC program is burdensome for small business.

The Rule should consider small business exemption for Level 2 third party assessments among second tier suppliers when a supplier is a small business and not receiving all of the data flowed

from government agency to the Prime. If the data is sensitive enough to require third party assessments at a sub-tier/subcontractor, the data should be marked and identified beyond CUI.

4. *"…However, an initial regulatory flexibility analysis has been performed and is summarized as follows:*
This proposed rule is necessary to respond to the threat to the U.S. economy and national security posed by ongoing malicious cyber activities designed to steal hundreds of billions of dollars of U.S. intellectual property…"

   Comment:

   The notion that the proposed rule is necessary to save "hundreds of billions of dollars of U.S. intellectual property" is somewhat disingenuous, as the U.S. Government does not properly and consistently mark and identify the data it wishes to protect.

5. *"The proposed rule has two objectives. One objective is to provide DoD with assurances that a defense industrial base contractor can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information shared with its subcontractors in a multi-tier supply chain. Another objective is to partially implement section 1648 of the NDAA for FY 2020."*

   Comment and Recommendation:

   Considerations should be made to third tier organizations on the supply chain. Analysis should be done on the effectiveness of this Rule to manage data from U.S. Government Agency to Prime to Subcontractor, and the Subcontractor's supply chain.

   Since access to SPRS is limited, a second-tier subcontractor machine shop would have no way of confirming eligibility of a finishing house outside of the finishing house's self-attestation of CMMC L1 (or L2 self-assessment) compliance. Additionally, it is unreasonable to think this added requirement check will be effectively performed within a growing list of requirements already on a small business list, while a manufacturer works to provide product for its larger Prime customers and ultimately DoD.

   Military leaders are focused heavily on meeting deadlines on manufactured equipment and parts for the aerospace and defense industry. There is far too much pressure on machine shops to ship a conforming part on time (or early). Expecting a sub-tier to have the leverage with its suppliers to now also manage CMMC flow-down to an already constricted and limited DIB is a futile attempt at controlling flow of CUI.

Thank you for the opportunity to provide Public Comment.

Sincerely,

Allison K. Giddens

Allison K. Giddens
President, Operations and Co-Owner
Win-Tech, Inc.