November 30, 2020

Submitted Via Email to osd.dfars@mail.mil.

Re: DFARS Case 2019-D041, Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements

The Coalition for Government Procurement (the "Coalition") appreciates the opportunity to comment on the Interim Rule in the above-referenced Defense Federal Acquisition Regulation Supplement ("DFARS") Case and, with these comments, seeks clarification from the Department of Defense ("DoD" or the "Department") regarding the process for implementation of Interim Rule.

By way of background, the Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Its members collectively account for a significant percentage of the sales generated through General Services Administration contracts, including the Multiple Award Schedule ("MAS") program. Coalition members also are responsible for many of the commercial item solutions purchased annually by the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for 40 years in promoting the mutual goal of common-sense acquisition.

The Coalition fully endorses the security objectives of the DFARS Interim Rule in seeking to enhance protection of unclassified information in the defense supply chain. As discussed more fully below, however, the Coalition recommends that the process for implementation of the Interim Rule be clarified so that contractors have a clearer sense of when they may have responsibilities under the rule (and what those responsibilities may be), and so that the rule is not so prohibitively expensive that innovative small businesses are forced out of the Defense Industrial Base ("DIB"). For these reasons, the Coalition urges that DoD take the following actions.

I. COMMENTS

A. DoD Should Clarify How the Assessment Processes Will Work.

1. DoD Assessment Process

The Interim Rule states that "[t]he Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST [National Institutes of Standards and Technology] SP [Special Publication] 800–171 DoD Assessment . . . if necessary." DFARS: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61,521 (Sept. 29, 2020). With regard to the Medium Assessment, the Interim Rule provides that such assessment consists of "[a] review

of a [C]ontractor's Basic Assessment;" "[d]iscussions with the contractor to obtain additional information or clarification, as needed;" and "[a] thorough document review;" that "[r]esults in a confidence level of 'Medium' in the resulting score." *Id.* Of the High Assessment, the Interim Rule states that such an assessment consists of "[v]erification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan," in addition to the other elements of the Medium Assessment. *Id.*

The Coalition requests that DoD provide additional information about how it will conduct Medium and High Assessments and how the assessment process otherwise will work. For example, can DoD specify what criteria it will use in its "[v]erification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan"? Does DoD anticipate that it will increase the number of Defense Contract Management Agency ("DCMA") assessors who support the DIB Cybersecurity Assessment Center ("CAC") program? Will DCMA, through DIB CAC, or otherwise, provide resources who can respond to contractor questions about the DoD Assessment Methodology?

The Coalition also asks whether DCMA will conduct Medium and High Assessments of service providers, systems integrators, or software developers, as well as supply contractors? If this is not a DCMA responsibility, who will assess such entities?

2. Potential Burden on Systems Integrators

The Interim Rule states that "[i]n order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment . . . for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order." *Id.* at 61,520. The Coalition is concerned with the burden that this requirement could put on systems integrators, some of whom, are members of the Coalition. Systems integrators bring together component subsystems and therefore, if subject to the Interim Rule, could be required to conduct an assessment for each of its component subsystems, which would be a time-consuming and expensive process. The Coalition thus urges DoD to consider the potential impact of this requirement on systems integrators.

3. Reciprocity

The Interim Rule states that "[t]he NIST SP 800-171 DoD Assessment will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) . . . except for rare circumstances when a re-assessment may be necessary . . . such as, but not limited to when there are indications of issues with cybersecurity and/or compliance with CMMC requirements." 85 Fed. Reg. 61,519–61,520.

Will DoD accept third-party audited/3PAO-certified NIST SP 800-53 Federal Information Processing Sandards-199 Moderate auditor attestations in place of NIST SP 800-171 self-attestations, as the NIST SP 800-53 standard is more rigorous than NIST SP 800-171 and is the very same standard the government itself is required to implement for its own information

systems? If so, the Coalition recommends that the final rule explicitly state this by modifying both DFARS 204.7302 (a)(5) and DFARS 252.204-7020 (d).

Similarly, the Interim Rule applies to, but does not contemplate, multi-national supply chains and foreign subsidiaries. The Coalition requests that DoD clarify how the Interim Rule applies to such entities.

4. DoD Rebuttal Process

The Interim Rule states that "DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS." *Id.* at 61,522. The Interim Rule further provides that, [u]pon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question." *Id.*

The Coalition requests that DoD provide additional information about this dispute resolution process. For example, what must a contractor submit to dispute its score? To whom? Who will decide whether, based upon additional information submitted, a contractor has sufficiently demonstrated that it meets the security requirements at issue or that it has rebutted the findings that may be in question?

B. DoD Should Streamline the Progression of Cybersecurity Maturity Levels

1. The CMMC Assessment

The preamble to the Interim Rule states that "DIB companies that do not process, store, or transmit CUI [Controlled Unclassified Information], must obtain a CMMC Level 1 certification," and that "DIB companies that process, store, or transmit CUI must achieve a CMMC level 3 or higher, depending on the sensitivity of the information associated with a program or technology being developed." *Id.* at 61,510. The preamble to the Interim Rule also states that a contractor "can seek to achieve Level 3 (without first achieving a Level 2 certification) if the necessary cybersecurity practices and processes have been implemented." *Id.* at 61,516.

It would be helpful to understand when DoD anticipates that it will release a CMMC assessment guide. Likewise, the Coalition also believes it would be helpful to understand what CMMC Levels will be covered by that guide.

Although contractors likely will not "process, store, or transmit," CUI until they must achieve a CMMC Level 3, the preamble to the Interim Rule indicates that DoD has retained CMMC Level 2, even though "the Department does not anticipate releasing new contracts that require contractors to achieve CMMC Level 2." 85 Fed. Reg. 61,516. If this statement is an acknowledgement that CMMC Level 2 is unnecessary, DoD should consider whether to remove

it from CMMC. Alternatively, the Coalition suggests that DoD could add more structure to CMMC Level 2. As explained in the preamble, CMMC Level 2 practices encompass only 48 of the 110 security requirements of NIST SP 800-171, as well as two process maturity requirements from the CMMC Model. *Id*. Would DoD consider making CMMC Level 2 available for companies that have sought, but not achieved, CMMC Level 3? For illustration, if a company failed to satisfy all Level 3 requirements, but does meet all those for Level 2, could it receive a Level 2 certification which would be accompanied by a statement of requirements that the company must meet for Level 3? Requiring activities may find it advantageous to have an opportunity to use a supplier with a Level 2 certificate knowing what is needed (and when) to step up to Level 3.

The preamble to the Interim Rule advises that it "estimates that the total the number of unique prime contractors and subcontractors is 220,966, with approximately 163,391 or 74 % being small entities . . . According to FPDS [the Federal Procurement Data System], the average number of new contracts for unique contractors is 47,905 for any given year." *Id*. The preamble also assumes that contractors seeking Level 1 "should have already implemented the 15 existing basic safeguarding requirements under FAR clause 52.204-21" and, for this reason, "there are no estimated nonrecurring or recurring engineering costs associated with CMMC Level 1." *Id*. at 61,513.

The Coalition believes that DoD, in this respect, greatly underestimates the burden and cost that will be imposed upon tens of thousands of smaller businesses, some of whom are Coalition members, as they seek confidence that they will obtain a Level 1 certification when the time comes that they are assessed. The Coalition further believes that the CMMC Model has its greatest importance, for DoD's purposes. DoD states that it "does not anticipate releasing new contracts that require contractors to achieve CMMC Level 2," thus making it unnecessary. Compliance, even with CMMC Level 1, likely will be expensive and disruptive for thousands of companies, though they do not possess any form of CUI. The Coalition believes that the expense and uncertainty of CMMC Level 1 and Level 2 coverage are disproportionate to actual security benefit and will prove painfully dilutive of scarce resources for assessment as well for implementation of needed security improvements. Accordingly, the Coalition urges DoD to consider postponing implementation of CMMC Level 1, recast or dispense with CMMC Level 2, and instead focus at the present time exclusively on CMMC Level 3.

Of Levels 4 and 5, the preamble to the Interim Rule states that "[t]he CMMC model includes additional processes and practices in Levels 4 and 5 that are focused on further reducing the risk of" Advanced Persistent Threats. 85 Fed. Reg. 61,509. Is there sufficient distinction between Levels 4 and 5 to warrant their separate articulation? Given the substantial cost of compliance with the higher CMMC maturity levels, the relatively small number of contractors that will be subject to CMMC Level 4 and Level 5, and the absence of accomplishment in accreditation or assessment methods for these levels, the Coalition urges DoD to delay implementation of CMMC Levels 4 and 5 until after the CMMC infrastructure is adequately built out and substantial functional experience has been gained with CMMC Level 3. While we recognize the challenge of more advanced threats and that higher-level security may be required

in some cases, the Coalition believes that, in the near term these issues can be dealt with on a program or contract basis.

2. Sufficient Availability of Assessors and C3PAOs

The preamble to the Interim Rule states that "[g]iven the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years." *Id.* at 61,510. "CMMC addresses the challenges of the Department scaling its organic assessment capability by partnering with an independent, nonprofit CMMC–AB that will accredit and oversee multiple third party assessment organizations (C3PAOs) which in turn, will conduct on-site assessments of DoD contractors throughout the multi-tier supply chain." *Id.*

The Coalition has observed evidence of progress on the part of the CMMC–AB in the training and accreditation of Provisional Assessors, but the numbers of such Provisional Assessors are small. For CMMC to assess even a small fraction of companies who may need a CMMC Level 3 certificate, much less the very much greater number of companies who now are subject to CMMC Level 1, there must be an enormous increase in the number of trained and accredited assessors and C3PAOs. When does DoD anticipate that it will have a sufficient number of assessors to move beyond the initial, "pathfinder" projects? Can DoD provide a schedule of what it anticipates from the CMMC–AB in numbers of assessors and C3PAOs between now and October 1, 2025, when the CMMC contract clause DFARS 252.204-7021 is to be included in all solicitations and contracts or task orders?

3. The CMMC Dispute Resolution Process

The Interim Rule states that "CMMC Assessments will be conducted by C3PAOs, which are accredited by the CMMC–AB," and that "C3PAOs will provide CMMC Assessment reports to the CMMC–AB." *Id.* at 61,513. The Interim Rule further states that "[t]he CMMC–AB will issue CMMC certificates upon the resolution of any disputes or anomalies during the conduct of the assessment." *Id.* Of disputes, the Interim Rule provides that "[i]f a contractor disputes the outcome of a C3PAO assessment, the contractor may submit a dispute adjudication request to the CMMC–AB along with supporting information related to claimed errors, malfeasance, or ethical lapses by the C3PAO." 85 Fed. Reg. 61,513. The Interim Rule also provides that "[t]he CMMC–AB will follow a formal process to review the adjudication request and provide a preliminary evaluation to the contractor and C3PAO" and "[i]f the contractor does not accept the CMMC–AB preliminary finding, the contractor may request an additional assessment by the CMMC–AB staff." *Id.*

What is the process a contractor must follow if it has a conflict with one of the assessors? The Coalition urges DoD to describe further the "formal process" that the CMMC–AB will follow "to review the adjudication request and provide a preliminary evaluation." *Id.* We also urge DoD to consider a tiered dispute resolution process in which the first tier is between the contractor and the CMMC—AB and the second tier is a DoD dispute resolution process. In this regard, we request DoD to advise industry on what roles and responsibilities it concludes must be retained and performed by DoD as "inherently governmental functions."

C. DoD Should Reassess the Cost of Implementing the Interim Rule on Contractors

The Interim Rule states that "[t]he estimated costs attributed to this rule do not include the costs associated with compliance with the existing cybersecurity requirements under the clause at FAR 52.204–21 or associated with implementing NIST SP 800–171 in accordance with the clause at DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," because "[c]ontractors who have been awarded a DoD contract that include these existing contract clauses should have already implemented these cybersecurity requirements and incurred the associated costs; therefore, those costs are not attributed to this rule." *Id.* at 61,511.

The Coalition is concerned that the conclusion that many contractors have already implemented these cybersecurity requirements and that, in fact, compliance with the existing cybersecurity requirements will be of no cost to contractors subject to the Interim Rule, is incorrect. The Coalition believes that DoD has miscalculated the cost of compliance with the Interim Rule and greatly understated the potential adverse financial impact upon many companies who are important participants in the DIB. In this regard, the Coalition is concerned particularly that the cost of compliance with the Interim Rule may be so prohibitive as to push some businesses out of the DIB market. Accordingly, the Coalition urges DoD to reassess the actual costs of compliance with the Interim Rule, taking into account both the DoD Assessment Methodology and the planned roll-out of CMMC requirements.

The Coalition also is concerned that there is an assumption inherent in the Interim Rule that the costs of compliance will be "allowable" costs. The Coalition does not fully understand the significance of this position since we would assume that costs reasonably required to satisfy a regulatory requirement, such as the Interim Rule, are allowable in any case. It is unclear, moreover, how such compliance costs can be recovered by contractors that do not have cost accounting systems in place, do not have forward pricing agreements or bill on a cost-reimbursement basis, or who supply on firm fixed-price contracts. The Coalition urges DoD to consider further how smaller and medium-sized companies, and those who do not perform on such "flexibly priced" contracts, as described above, can recover the costs of compliance. The Coalition recommends that DoD consider additional ways to limit the burden of CMMC implementation, particularly for contractors that do not receive any CUI. For example, where appropriate, contractors providing commercial services to support commercial-off-the-shelf ("COTS") items (like technical support for software) should receive the same exception as other COTS contracts.

D. DoD Should Consider Ways in Which It Can Adjust the Interim Rule to Better Accommodate New, Cheaper, and Better Methods and Technology

The Interim Rule is built around the controls of NIST SP 800-171, for the DoD Assessment Methodology, and then upon the practices and processes of the CMMC Maturity Model. In part, because we are concerned about the cost impact to many defense suppliers and sources, the Coalition urges DoD to identify, explore, promote, and accommodate new tools,

techniques, and technologies that can assist companies in the DIB to achieve the objectives of the Interim Rule more quickly and at much lower cost than under the *status quo*. Doing so is especially important if the Department is to maintain its ability to attract and retain non-traditional, innovative, and small businesses. As concerns cloud service, the Coalition believes that the Interim Rule should be revised to encourage cloud services, including managed security as a service and managed service providers, with sufficient security. The Coalition recognizes the value of FedRAMP to the authorization of cloud for federal information system purposes. At the same time, the Coalition urges DoD to assure that the process envisioned under CMMC is not duplicative, and that the Department remains open to all means available to demonstrate "equivalent" security.

II. CONCLUSION

The Coalition hopes you find these comments useful and thanks you for your time and consideration. Should you have any questions or concerns, please contact the undersigned at RWaldron@thegp.org or 202-331-0975.

Sincerely,

Roger Waldron
President