November 30, 2020

Via osd.dfars@mail.mil

Ellen M. Lord
Under Secretary of Defense Acquisition and Sustainment
c/o Heather Kitchens
Department of Defense
Washington, DC 20301

Subject: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

Dear Under Secretary Lord:

The U.S. Chamber of Commerce welcomes the opportunity to provide the Department of Defense (DoD) with feedback on its interim rule (the IR or the rule) to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to assess and verify the ability of DoD contractors to protect controlled unclassified information (CUI) on their information systems. The IR establishes two main lines of effort—a standard DoD assessment methodology and a Cybersecurity Maturity Model Certification framework (CMMC), which is expected to validate contractors' implementation of DoD-required cybersecurity practices and processes.[1]

Key Points

- The U.S. Chamber of Commerce believes that the Department of Defense's (DoD's) stated "crawl, walk, run" approach to rolling out the Cybersecurity Maturity Model Certification framework (CMMC) is sound. Many defense contractors are working hard to understand what the interim rule (IR) mandates, including conducting self-assessments of NIST 800-171 security controls and wrestling with many that the IR does not seem to address.

- Contractors have ongoing questions about appropriately identifying and marking CUI—short for controlled unclassified information—which DoD and industry should dedicate much time to working through.

- The Chamber appreciates the nuances that come with implementing the CMMC, including reimbursing contractors' cybersecurity costs. The IR notes that CMMC expenses will rest on several factors (e.g., a contractor's CMMC level, the complexity of the company's network, and other market forces). Too often overlooked, contractors are battling nation states and their proxies that are amply funded to target CUI for theft and misuse. The Chamber wants to ensure government contractors receive just reimbursement as they implement measures to meet CMMC requirements.

- The CMMC's goal is to improve the cybersecurity of the defense industrial base, specifically reducing the risk of unauthorized access of CUI by foreign powers. A process should be established that identifies a subset of anonymized assessment/certification data that appropriate stakeholders can analyze with DoD oversight to measure whether the CMMC leads to a reduction in risk. A relatively open, scientific way of analyzing the CMMC is necessary to assess if it works (i.e., measurably reduces CUI theft).

- DoD is urged to coordinate with Congress, agencies, and industry to push increased coherence to the proliferation of federal supply chain risk management initiatives that are underway, including streamlining existing cyber-related regulations with the CMMC. The Chamber's constructive discussions with DoD suggest that a number of cybersecurity programs, standards, and/or models are slated for reciprocity with the CMMC. This effort is a step in the right direction, and we look forward to engaging DoD in follow-up activities.

The Chamber believes that DoD's stated "crawl, walk, run" approach to rolling out the CMMC, which will become the beating heart of the rulemaking, is a sound way to proceed. A dominant takeaway we have is that many contractors are working hard to understand what the IR demands of them, including executing near-term requirements (e.g., completing the basic self-assessment pursuant to DFARS clause 252.204-7012)[2] and wrestling with a number of questions that the IR does not appear to fully address.[3]

The Chamber offers input on important themes and specific issues that have been underscored by several business groups and invites follow-up discussions with the department. Worth stressing, DoD should coordinate with Congress, agencies, and industry to push increased coherence to the proliferation of federal supply chain risk management initiatives that are underway.[4]

Answering ongoing and fundamental CUI questions. DoD contractors of all sizes have continuing, yet fundamental, questions about CUI, which is an umbrella term for all unclassified information that requires safeguarding under Executive Order 13556. A governmentwide CUI Registry provides information on the specific categories and subcategories of information that the executive branch guards closely.[5] Still, the scope of CUI marking is a leading concern that the Chamber consistently hears from contractors, and it should be a central one that DoD and industry spend more time working through.

It seems that DoD marks some digital and physical documents as CUI, but contractors are largely responsible for determining whether sensitive, unclassified information in their possession (e.g., paper documents) is CUI. DoD says, "Contractors must mark or otherwise identify … [in accordance with the contract], DoD CUI that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract."[6] Despite the availability of government aids and related materials to coach contractors on CUI, the level of uncertainty that businesses have expressed to us is too high. One business representative remarked that CUI is "the game," stressing that DoD and industry must have mutual recognition of what is/isn't CUI if the CMMC is to get off the ground. DoD leadership should feel similarly and work with contractors and organizations like the Chamber to remedy businesses' queries.

Indeed, some crucial questions regarding CUI that the Chamber consistently receives from members are—

- Will additional materials (e.g., sector-specific guidance) be provided to contractors? Materials that have been published to date don't seem to meet contractors' needs. The Chamber appreciates that DoD is planning to work with the energy sector, among others, on identifying and marking CUI proficiently, which is a step in the right direction.

- Which agencies besides DoD will mark information as CUI? Contractors are urging DoD to provide a clear and consistent definition of CUI to implement the rule.

- How does DoD plan to ensure that all organizations within the department, including the service branches,[7] will employ the same approach to identifying/marking CUI?

Paying for DoD and contractor cybersecurity. The Chamber appreciates many of the nuances that come with promulgating the CMMC, including reimbursing aspects of contractors' cybersecurity costs. DoD reports that the aggregate loss of CUI from the defense industrial base (DIB) increases risks to U.S. economic prosperity and national security. To reduce these risks, the IR requires defense contractors to assess, document, and store within DoD (i.e., the Supplier Performance Risk System or SPRS) the results of their assessments as a means of enhancing their cybersecurity and protecting CUI on their networks.[8]

A fundamental challenge with cybersecurity is recognizing what programs and practices to undertake, and another one is paying for them. Many policymakers reasonably want contractors to institute strong network security practices and data protection measures, but sometimes it seems that government is unable or unwilling to pay for them. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, already mandates that certain contractors "implement" all 110 security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (NIST 800-171), to protect CUI.[9]

DoD suggests in the IR that the government has essentially paid for existing requirements that are underpinning the new CMMC.[10] The Chamber appreciates DoD's thinking on this issue, although we want to engage department officials on fully reimbursing contractors for mandated data protection measures that are expansive under current and pending rules like the CMMC. For example, the CMMC requires contractors pursuing a level-3 certification to implement the existing 110 NIST 800-171 controls, plus 23 new ones (20 practices and 3 processes). The Chamber's understanding is that DoD will consider the costs of these additional requirements as allowable costs associated with the performance of a contract.[11] Getting DoD and government contractors increasingly on the same page regarding this issue is critical, especially as contractors are dealing with the economic effects of COVID-19.

In addition, the initial implementation of the CMMC will only be within DoD,[12] but it may migrate to civilian agencies and greatly expand the costs and related burdens of implementation across a wider swath of the U.S. industrial base. This is concerning to the Chamber, and we urge decision makers to engage in an extensive dialogue with industry partners before expanding the scope of CMMC beyond DoD.

According to the IR, the CMMC's five maturity levels range from basic cybersecurity hygiene (level 1) to advanced/progressive (level 5). DoD views CMMC level 1 as a basic information security program for safeguarding federal contract information. Level 2 is considered to be a transitional step toward meeting level 3, which is when the protection of CUI kicks in.[13] According to the rule, contractors that process, store, or transmit CUI must achieve a CMMC level of 3 or higher.[14] CMMC levels 3–5 require contractors to implement all 110 security requirements specified in NIST 800-171, and more.

The CMMC also incorporates practices and processes from other standards, references, and/or sources (e.g., NIST SP 800-53, Aerospace Industries Association National Aerospace Standard 9933, Critical Security Controls for Effective Capability in Cyber Defense, and Computer Emergency Response Team Resilience Management Model version 1.2.).[15]

The Chamber anticipates that there will be some disparities among contractors in their level 3 readiness, which will be addressed through a contractor's POA&Ms—which is short for plans of action and milestones—describing how and when unimplemented security requirements will be met.[16] The Chamber is not clear if Congress and DoD will pay for contractors' investments under the CMMC with the funds needed to both implement and maintain the required 17 (level 1), 72 (level 2), 130 (level 3), 156 (level 4), or 171 (level 5) security practices.[17]

The Chamber is troubled by DoD and related surveys that highlight contractors' continued challenges in achieving widespread implementation of cybersecurity requirements (e.g., NIST 800-171). On the one hand, a sizeable number apparently lacked awareness of DFARS 252.204-7012. On the other hand, close to 40% of contractors in the high-assessment category, which DoD conducts on-site, demonstrated compliance with all 110 NIST 800-171 controls.[18] The Chamber wants to work with DoD to more accurately discern if funding is a leading factor in contractor compliance issues. To date, we are unaware of peer-reviewed consensus data that satisfactorily answer this question.

The Chamber contends that the relationship between resources and compliance/noncompliance needs to be explained more completely before we embark on the CMMC. We want contractors to meet their security requirements, but DoD culture plays a central role in performance outcomes. According to a popular study, DoD's "historical emphasis on 'cost, schedule, and performance' is a fundamental driver for actions of DoD as well as the DIB." Increasingly, DoD leadership recognizes that the department's acquisition structure rewards cost, schedule, and performance more than integrated risk management capabilities such as contractor cybersecurity.[19]

DoD notes in the rule that CMMC costs will depend upon several factors, such as a contractor's CMMC level, the complexity of the company's network, and other market forces.[20] What is often overlooked, defense contractors are battling nation states and their proxies that are amply resourced to target CUI for theft and misuse. The Chamber urges the administration and DoD to work closely with Congress to properly fund the CMMC. We want contractors to meet their CMMC requirements and receive fair compensation. By achieving this goal, the U.S. will improve its defenses against adversaries' asymmetric operations against the DIB and impose costs on such actors/activities.[21]

Balancing the security and transparency of assessment/certification data to measure whether the CMMC works. The Chamber has mixed views on CMMC Third Party Assessment Organizations (C3PAOs) and the CMMC Accreditation Body. Businesses often want to withhold examination reports to certain recipients, especially to protect sensitive data from third parties (e.g., regulators) and malicious actors. While a dialogue with DoD has started, more communication between the department and industry is needed to better know how the assessment/certification data will be assembled, used, protected, and shared by the government. The security and appropriate sharing of CMMC data are top Chamber priorities.

The Chamber understands that the C3PAOs, certified assessors, the Defense Contract Management Agency (DCMA), the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), and contracting officers will have primary, if not sole, access to the collected assessment/certification data of contractors. The Chamber wants to make sure that assessment/certification data are safeguarded, but the data should undergo rigorous peer review with DoD oversight so that the CMMC is constructively critiqued, with the findings driving measurable improvements in DIB cybersecurity.

Certain organizations, including the C3PAOs and elements of DoD, should not have a monopoly on using the assessment/certification information.[22] The Chamber urges DoD to consult closely with its contracting community about the trade-offs involved in both protecting CMMC data and analyzing them to reduce uncertainty and bolster DIB cybersecurity.

The stated goal of the CMMC is to improve the cybersecurity of the DIB, particularly reducing the risk of unauthorized access of CUI by foreign powers. A process should be created identifying a subset of anonymized assessment/certification data that appropriate U.S. stakeholders can analyze to measure whether the CMMC leads to a reduction in risk. What this means is that the probability and/or the loss of CUI to America's adversaries decreases. Such an effort will take thoughtful deliberation and time. Nonetheless, initially, even small reductions in DoD and contractor uncertainty about risks to protected CUI can be valuable.

DoD officials and contractors need to make tough decisions about prudently allocating taxpayer and business monies, especially with respect to instituting certain controls, which cannot be based on expert intuition or best practices alone. The IR mandates that contractors apply specific controls, and these controls cost money.

In sum, the Chamber believes that a relatively open, scientific way of analyzing the CMMC will be necessary. The CMMC will be said to "work" if it measurably reduces the risk of

CUI theft compared with alternative methods. The last thing that DoD (presumably) and the Chamber want is for "compliance" with the CMMC to amount to going through the regulatory motions. A permissible range of stakeholders should be able to independently measure the risk assessment methods that underly the framework. If complying with the CMMC does not measurably enhance risk management, then the program should change. It is unclear to the Chamber how CMMC performance will be measured, and how it will be known whether risks have decreased or increased.[23]

Streamlining regulations and reciprocity. For several years, policymakers of both parties have wanted to "align, leverage, and deconflict" policies, laws, and regulations to increase U.S. cybersecurity through improved efficiency.[24] However, progress is still largely aspirational. Depending on the service or type of products that DoD contractors, they are likely subject to multiple requirements, assessments, and certifications across the federal government. Cloud service providers, for instance, are required to meet many conditions in DoD's *Cloud Computing Security Requirements Guide* and the Federal Risk Authorization and Management Program (FedRAMP). The Chamber urges DoD to help policymakers and industry streamline existing cyber-related regulations to meet both DFARS clause 252.204-7012 and the CMMC requirements. Based on the Chamber's constructive discussions with DoD principals, the programs listed below are slated for reciprocity with the CMMC and are expected to be posted online—

- FedRAMP (moderate/high impact level).[25]
- International Organization for Standardization/International Electrotechnical Commission 27001 family.[26]
- Department of Energy Cybersecurity Capability Maturity Model.[27]
- DCMA DIBCAC (high confidence audit).

To facilitate reciprocity and serve the interests of DoD and contractors, CMMC maturity levels need to be clearly mapped to these cybersecurity programs. The mapping of the programs' equivalent certification levels to CMMC levels should be stated in writing and in agreements commonly throughout DoD and other federal bodies.[28]

Addressing additional process and organizational issues. DoD is urged to address several key procedural and organizational issues that affect the department and contractors under the rule.

- **Securing and readying SPRS.** Industry groups want to understand how DoD will protect the basic assessment information that contractors must submit to SPRS, which could be sensitive when consolidated, and what mitigations DoD will employ if SPRS is not ready by November 30, 2020. Will SPRS, for example, have all the fields needed for contractors to submit the information mandated in the IR, and will submissions require multifactor authentication?

- **Correcting temporary assessment deficiencies.** The IR does not seem to offer contractors enough clarity on how quickly entities should correct deficiencies in meeting the NIST 800-171 controls and complete POA&Ms,[29] as well as request exceptions for government-furnished equipment and/or contractually mandated requirements.

- **Wrestling with incident response obligations.** Some controls, such as having a security operations center with a 24/7 incident response capability, may not be achievable for many businesses, particularly small and midsize firms. Will incident response capabilities be required for all contractors regardless of size and resources?

- **Having one or more certifications.** The IR says, "A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted."[30] Industry seeks additional confirmation that it is acceptable for contractors (e.g., multinationals) with multiple business segments to get one or more CMMC classifications (e.g., one part could require a level 1 certification; another part could require a level 3 certification). Or will the highest CMMC level be applied to the whole enterprise?

- **Clarifying the definition of COTS.** The IR says companies that solely produce COTS, or commercial-off-the-shelf, products do not require a CMMC certification, which the Chamber supports. Still, to further increase consistency and reduce some confusion in industry, the Chamber urges DoD to issue departmentwide guidance clarifying that the definition of COTS for assessment and CMMC purposes is the same as the one (i.e., "commercially available off-the-shelf (COTS) item") under FAR 2.101 definitions (FAR part 2, subpart 2.1, section 2.101).[31]

***

The Chamber appreciates the opportunity to provide you and your DoD colleagues with comments on the IR. If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Endnotes

[1] Defense Acquisition Regulations System, Department of Defense (DoD), Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), *Federal Register*, September 29, 2020. https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of

[2] DoD, NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020 (DoD Assessment Methodology). https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf

[3] See Susan B. Cassidy et al., "Department of Defense's Interim Rule Imposes New Assessment Requirements But is Short on Detail on Implementation of CMMC," Covington & Burling LLP, October 6, 2020. The article describes well the current regulatory landscape and the basics of the DoD assessment methodology and the Cybersecurity Maturity Model Certification framework (CMMC), as well as flags several of the rule's open questions. https://www.insidegovernmentcontracts.com/2020/10/department-of-defenses-interim-rule-imposes-new-assessment-requirements-but-is-short-on-detail-on-implementation-of-cmmc/?_ga=2.94641050.745563625.1606174191-958316305.1606174191

[4] Cyberspace Solarium Commission, *Building a Trusted ICT Supply Chain*, October 19, 2020, pp. ii, 7. https://www.solarium.gov/public-communications/supply-chain-white-paper

See the U.S. Chamber of Commerce's November 2, 2020, letter to the Office of Management and Budget and the Federal Acquisition Security Council on the interim final rule to implement the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) (P.L. 115-390). https://www.uschamber.com/sites/default/files/11-2-20_uscc_letter_fasc_ifr_final_v1.pdf

[5] https://www.archives.gov/cui

[6] DoD Assessment Methodology, p. 2.

[7] https://www.defense.gov/Resources/Military-Departments

[8] Cybersecurity Maturity Model Certification (CMMC) frequently asked questions (FAQs) #3, https://www.acq.osd.mil/cmmc/faq.html

[9] https://www.acquisition.gov/dfars/part-252-clauses#DFARS-252.204-7012

[10] FR 61513–61514.

[11] FR 61514.

[12] CMMC FAQs #7.

[13] The CMMC applies to only a defense industrial base (DIB) contractor's unclassified networks that handle, process, and/or store federal contract information (FCI) and/or CUI. If a DIB company does not

possess CUI but possesses FCI, it is required to meet FAR clause 52.204-21 and must be minimally certified at CMMC level 1. FAQs #19 and #22.

[14] FR 61510.

[15] CMMC FAQs #8.

[16] FR 61508.

[17] https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

[18] FR 61518.

[19] Chris Nissen et al. *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, MITRE, August 2018, pp. 10, 19. https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security

[20] CMMC FAQs #11.

[21] Jason Healey, "A Bizarre Pair: Counterinsurgency Lessons for Cyber Conflict," *Parameters* 50, no. 3 (2020). https://press.armywarcollege.edu/parameters/vol50/iss3/9

[22] Eli Berman et al. *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton University Press, 2018), pp. 314–316.

[23] Douglas W. Hubbard and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk* (Wiley, 2016), pp. 28–29, 34, 52, 190, 234.

[24] See, for example, the Chamber's July 2016 letter to Cybersecurity Forum for Independent and Executive Branch Regulators. https://www.uschamber.com/sites/default/files/u.s._chamber_letter_to_cyber_forum_july_8_final.pdf

[25] https://www.fedramp.gov/understanding-baselines-and-impact-levels/

[26] https://www.iso.org/isoiec-27001-information-security.html

[27] https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program

[28] See also the November 30, 2020, Council of Defense and Space Industry Association (CODSIA) letter (p. 3) to DoD on the IR, which was in draft form at the time of this writing.

[29] FR 61518.

[30] FR 61505.

[31] November 30, 2020, CODSIA letter (p. 2) to DoD.