Before the
U.S. Department of Defense
Washington, DC 20301

In the Matter of	)	
	)	
Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements	)	Docket DARS–2020–0034
	)	
	)	RIN 0750–AJ81
	)	
	)	
DFARS Case 2019–D041	)	

COMMENTS OF USTELECOM—THE BROADBAND ASSOCIATION

I. INTRODUCTION

USTelecom—The Broadband Association ("USTelecom")[1] and its members are world leaders in cybersecurity, and we have compelling long-term interests in working with the Department of Defense ("DoD") to ensure that the Cybersecurity Maturity Model Certification ("CMMC") becomes a powerful lever for security innovation and supply chain assurance in government contracts and private commercial transactions, rather than a check-the-box exercise. Given DoD's reach and influence, the CMMC is a foundational initiative with broad long-term implications in cybersecurity and supply chain security, and it is crucial that DoD work with private sector security leaders to get this right.

To that end, we suggest four general areas of recommendation. The CMMC should:

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives — all providing advanced communications service to both urban and rural markets.

1. Account for differences in various types of contract services, to include implementing principles that apply to commercial off the shelf ("COTS") procurement and "plain old telephone service" ("POTS") contracts.

2. Provide mechanisms for timing and implementation that incentivize ever-improving cybersecurity rather than static one-time certifications.

3. Work with other federal agencies to apply the CMMC on a consistent basis throughout the federal government and ensure whole-of-government coordination on cybersecurity and supply chain assurance.

4. Leverage other existing programs such as FedRAMP for purposes of reciprocity and coherent application across the federal government.

USTelecom and its members stand ready to work with DoD to implement the CMMC, and we welcome this opportunity to provide our input on the interim final rule.

II. USTELECOM AND ITS MEMBERS ARE WORLD LEADERS IN CYBERSECURITY, AND WE HAVE COMPELLING LONG-TERM INTERESTS IN WORKING WITH THE DEPARTMENT OF DEFENSE TO ENSURE THAT THE CMMC BECOMES A POWERFUL LEVER FOR SECURITY INNOVATION AND SUPPLY CHAIN ASSURANCE.

For decades, USTelecom and its members have played a prominent leading role in the security, resiliency and innovation of the U.S. communications infrastructure, in close and collaborative partnership with the U.S. government. USTelecom helped the National Institute of Standards and Technology ("NIST") develop the Cybersecurity Framework, and we led the Federal Communications Commission ("FCC") Communications Security, Reliability, and Interoperability Council's ("CSRIC") landmark effort to implement the Framework in the communications sector.

USTelecom also chairs both the Communications Sector Coordinating Council ("CSCC") and the Department of Homeland Security ("DHS") Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force, the two principal organizations that serve as the government's industry partners for developing cybersecurity and supply chain security policies. The roots of the CSCC and its partner organizations – the

National Coordinating Center for Telecommunications ("NCC") and the Communications Information Sharing and Analysis Center ("Comm ISAC"), both housed in DHS – reach back to the government's need for industry expertise and support in addressing nuclear threats to government communications and continuity of operations during the Cold War era.

Likewise, the President's National Security Telecommunications Advisory Committee ("NSTAC"), established by President Ronald Reagan via executive order at the height of the Cold War in 1982, has provided six Presidents U.S. industry's best expertise and recommendations for national security and emergency preparedness communications. NSTAC's most recent report[2] evaluated the nation's ICT infrastructure resilience during the increased connectivity demands of the early months of the COVID-19 pandemic (roughly the five months from March through July). The report found that due to a variety of positive response factors – for instance, significant capital investments, business continuity and work-from-home planning, diversity in ICT supply chains, and information sharing and response coordination – providers responded well to the pandemic's unprecedented demands. In the words of the report, "the overall ICT ecosystem response to the pandemic was strong."

The NSTAC report found that the ICT ecosystem's robust response to the pandemic was a result of private sector investment and innovation, leveraged for security and resilience through partnership with the government. In short, since the existential nuclear threats of the Cold War, the U.S. government has recognized that the world's most secure and resilient networks are those that are owned and operated by U.S. private industry. We wish to bring this expertise and spirit of partnership to DoD's important effort to implement the CMMC.

[2] Letter from NSTAC Chair, John Donovan, to President Donald Trump, The White House, *available at* https://www.cisa.gov/sites/default/files/publications/NSTAC%20Letter%20to%20the%20President%20on%20Communications%20Resiliency%20.pdf.

III. IT IS CRUCIAL THAT DOD WORK WITH USTELECOM AND ITS MEMBERS, ALONG WITH OTHER PRIVATE SECTOR SECURITY LEADERS, TO GET THE CMMC PROGRAM RIGHT.

In addition to the above public-private initiatives, USTelecom members are also key suppliers of contract services to DoD. It is in our core long-term and direct interests that DoD gets this important program right to ensure that the CMMC leads to security innovation and supply chain assurance for DoD suppliers and beyond. To that end, we offer the following four general areas of recommendation.

A. The CMMC should account for differences in various types of contract services, to include implementing principles that apply to COTS procurement and POTS contracts.

Unless a contract provides a specialized service that is specific to DoD's unique national security needs, basic commercial voice and data transport services should be treated as COTS. The CMMC's certification requirements are generally intended for security assurance across all of DoD's thousands of contractors; this is not necessary for providers of commercial telecom service, who, as described above, have been world leaders and government partners in communications security for decades. DoD has already spoken to this issue generally in the context of POTS, and this principle should apply generally to all commercial telecommunications services provided to DoD.[3]

[3] *See* Department of Defense Procurement Toolbox, *Frequently Asked Questions*, *available at* https://dodprocurementtoolbox.com/faqs/cybersecurity ("**Q103:** Regarding security requirement 3.13.8– How is CUI to be protected when transmitted over Common Carrier telecommunications lines/Plain Old Telephone Service (POTS)? **A103:** Common Carrier telecommunications circuits or Plain Old Telephone Service (POTS) would not normally be considered part of the information system processing CUI. Data traversing Common Carrier systems should be separately encrypted per 3.13.8. Contracts with Common Carriers to provide telecommunications services may include DFARS clause 252.204-7012, but should not be interpreted to imply the Common Carrier telecommunications systems themselves have to meet the DFARS requirements. Data transmission of CUI transmitted over standard telephone dial-up service (POTS) similarly should be separately encrypted as no protection is expected to be provided by the telephone system. Voice communication of CUI over the telephone is not addressed by NIST SP 800-171 or by DFARS clause 252.204-7012.").

Moreover, commercial telecommunications services should be considered COTS since they are customer-agnostic; that is, apart from the cloud services governed by FedRAMP, there are no federal-specific commercial telecommunications services. We also note that services governed by the Telecommunications Act of 1996 are exempted from application of the Service Contract Act and the associated wage determinations.

Beyond this general principle regarding commercial telecommunications services, it is important that CMMC clarify how controlled unclassified information ("CUI") controls apply to Internet service providers ("ISPs") and foreign recipients. The global service model for the telecommunications industry is the "follow the sun" principle which enables 24x7 live support. CMMC (Level 3+) would limit this service model because of the prohibition of foreign dissemination for DoD CUI. There are two different types of data at issue: (1) DoD CUI data, and (2) transported data. It is crucial the CMMC account for and clarify these different types of data in its dissemination controls, particularly as they pertain to ISPs, that transport data controls do not work for global companies that transport data.

B. The CMMC should provide for timing and implementation that incentivize ever-improving cybersecurity rather than static one-time certifications.

The CMMC should recognize – and encourage – dynamic progress toward greater cybersecurity and supply chain assurance. To this end, implementation should allow an "on-ramp" to certification for qualified bidders, rather than certification prior to bidding. Such an implementation process would simultaneously reduce unnecessary barriers to entry and provide strong incentives for cybersecurity improvements among DoD contractors.

Additionally, given the present paucity of auditors qualified to perform CMMC audits, the CMMC must allow flexibility to account for auditor delay. Consistent with DFARS 252.204-7012, the CMMC should allow a Plan of Action and Milestones ("POAMs") for a 3-

year acquisition cycle. (We suggest that these POAMs be called "C-POAMs.") The Defense Contract Management Agency ("DCMA") will be auditing Medium and High Assessments against such POAMs so arguably there is a larger field of subject matter experts to perform these audits in the proposed 3-year period.

C. DoD should work with other federal agencies to apply the CMMC on a consistent basis throughout the federal government and ensure whole-of-government coordination on cybersecurity and supply chain assurance

As we have argued in other proceedings,[4] whole-of-government coordination and coherence in cybersecurity and supply chain assurance is crucial to promoting a diverse, competitive market of trusted ICT suppliers. We believe that a foundational supply chain regime must be built with solid cornerstones that include industry partnership; rigorous, discerning risk analysis; clear definitions of terms; and interagency coordination pursuant to a sound, fair, and predictable process.

The General Services Administration's ("GSA") recent reference to CMMC in the STARS III context illustrates the real possibility for wide application of the CMMC.[5] GSA noted that it "reserves the right" to require CMMC certifications for businesses that are awarded spots on the $50 billion governmentwide STARS III IT contracts.

To promote the coherence of the "whole of government" approach to ICT supply chain security and to maximize the impact of industry's real-world implementation of ICT supply chain risk management measures, we strongly recommend that DoD work closely with other

[4] *See* Comments of USTelecom, WC Docket No. 18-89, Federal Communications Commission (filed Feb. 3, 2020); Comments of USTelecom, Docket No. 191119-0084, RIN 0605-AA51, Department of Commerce (filed Jan. 10, 2020).

[5] *See, e.g.*, CMMC requirements show up in GSA's STARS III contract, July 8, 2020, *available at* https://www.fedscoop.com/newsletter/07092020-cmmc-requirements-show-up-in-gsas-stars-iii-contract.

agencies with the express intent of coordinating the respective various programs and requirements pertaining to the CMMC.

D. The CMMC should leverage other existing programs such as FedRAMP for purposes of reciprocity and coherent application across the federal government.

We are encouraged that DoD officials have indicated that the CMMC will allow for reciprocity with other regimes such as FedRAMP.[6] Developing reciprocity arrangements will provide a meaningful vehicle for the coordination and consistent application we advocate for above. Likewise, in the interest of consistency with other federal procurement norms, the final rule should flow down to subcontractors only when the prime contract includes a consent to subcontract requirement. Subcontractors that fall under a FAR Part 44 contractor purchasing system review ("CPSR"), as audited by DCMA, are already covered by the required DFARS 252.204-7012 flow down. Therefore, subcontractors within a CPSR are already verified regarding the implementation of the NIST SP 800-171 controls.

IV. CONCLUSION

The CMMC is a foundational initiative with broad long-term implications in cybersecurity and supply chain security. For instance, the ICT Supply Chain Risk Management Task Force Working Group 4's template of supply chain questions for buyers to inquire of vendors includes an explicit reference to the CMMC. This means that the CMMC could eventually become proxy for the cybersecurity-related vetting of vendors in purely private commercial transactions. Given the broad reach of DoD procurement and the still broader potential for ripple effects of the CMMC in private commercial supply chain security vetting, it

[6] *See, e.g.*, Lauren C. Williams, *What CMMC will mean for defense contractors*, FCW (Nov. 15, 2019), *available at* https://fcw.com/articles/2019/11/15/arrington-dod-cmmc.aspx (quoting Katie Arrington, DoD's Chief Information Security Officer for Acquisition and Sustainment, as stating to industry stakeholders, "I think that there's a lot of reciprocity to be had [with FedRAMP] because it's an investment that you've already made.").

will be important to ensure that the CMMC's implementation does not inhibit flexibility or innovation in ICT products and services, and that it does not trend over time toward a prescriptive checklist for cybersecurity.

USTelecom and its members are eager to work with you to implement this program in a manner that allows it to reach its potential to influence security and supply chain assurance for DoD and the broader federal and commercial ecosystem.

Respectfully submitted,

/s/
Robert Mayer
Senior Vice President, Cybersecurity
(202) 326-7300

/s/
Michael Saperstein
Vice President, Strategic Initiatives & Partnerships
(202) 326-7300

USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001