Before the
DEPARTMENT OF DEFENSE
DEFENSE ACQUISITION REGULATIONS SYSTEM
Washington, D.C. 20554

In the Matter of	)	
	)	
Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements	)	DFARS Case 2019-D041

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

November 30, 2020

TABLE OF CONTENTS

Before the
DEPARTMENT OF DEFENSE
DEFENSE ACQUISITION REGULATIONS SYSTEM
Washington, D.C. 20554

In the Matter of	)	
	)	
Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements	)	DFARS Case 2019-D041
	)	
	)	

COMMENTS OF CTIA

CTIA[1] welcomes the opportunity to comment on the Department of Defense's ("DoD" or "Department") interim final rule ("IFR" or "Interim Rule") putting into effect assessment methodologies for contractor implementation of cybersecurity requirements and protection of DoD unclassified information.[2] First, DoD will require contractors to complete a self-assessment of compliance with National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 starting November 30, 2020.[3] DoD will also begin to apply the Cybersecurity Maturity Model Certification ("CMMC") requirements.[4]

[1] CTIA – The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, and suppliers, as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, 85 Fed. Reg. 61505 (Sept. 29, 2020), https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of ("IFR").

[3] *See NIST Special Publication 800-171, Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf ("NIST SP 800-171").

[4] IFR at 61505.

CTIA and its members across the wireless ecosystem take pride in providing reliable, secure, and innovative communications services to the government, including DoD, directly and as service providers to other government contractors. The industry has a long history supporting the diverse voice and data service needs of the United States, from the first wireless services to 4G. CTIA's members look forward to bringing the promise of 5G and advanced services to government partners, including all parts of DoD. The government's purchase of innovative commercial telecommunications and data services provide it immense value.

In these comments, CTIA provides recommendations to the Federal Acquisition Regulation ("FAR") Council to ensure that new assessment methodologies are applied efficiently and consistently across the federal enterprise, with appropriate recognition for the unique characteristics of modern wireless communication services. CTIA's suggestions are intended to promote the Government's ultimate goal of safeguarding DoD's technologies and information.

I. INTRODUCTION & SUMMARY

CTIA's members include some of the world's largest wireless carriers and manufacturers. These companies provide sophisticated voice, data, and cloud-based services to the federal government, including to DoD[5] and numerous civilian agencies,[6] under various contracts. These

[5] For example, "Maxwell Air Force Base in Montgomery, Alabama has been working with AT&T to improve base security and force protection using the latest technology." *The Defense Network of Tomorrow—Today*, AT&T, at 3 (2018), https://www.business.att.com/content/dam/attbusiness/reports/industries-public-sector-federal-dod-network-of-future-white-paper.pdf.

[6] For example, AT&T and Verizon received a three-year Authority to Operate ("ATO") in March 2019 under the General Service Administration's ("GSA") Enterprise Infrastructure Solutions ("EIS") contract. *See EIS Business Support Systems Security Assessment and Authorization Announcement*, GSA Interact (Mar. 25, 2019), https://interact.gsa.gov/blog/eis-business-support-systems-security-assessment-and-authorization-announcement-0. *see also Enterprise Infrastructure Solutions (EIS)*, AT&T, https://www.business.att.com/industries/family/public-sector/enterprise-infrastructure-solutions.html; *Enterprise Infrastructure Solutions (EIS)*, Verizon, https://enterprise.verizon.com/solutions/public-sector/federal/contracts/eis/. Sprint supports the government through the GSA by providing the Federal Relay Service "for Federal employees who are deaf, hard of hearing, deafblind, blind and low vison, or have speech disabilities." *See Federal Relay Services*, Sprint, https://www.sprintrelay.com/services/federal-relay-services. Under the Navy's Spiral 3 Wireless and Telecommunications Services contract, "T-Mobile is providing 70,000 lines of wireless service to the U.S.

telecom and data services fall into a unique space when it comes to government contracts. Telecom and data service providers, including CTIA's members, participate in the federal procurement process across government missions as prime contractors and subcontractors. Due to the nature of the services they provide, they are also regulated by independent agencies such as the Federal Communications Commission ("FCC"). This regulatory oversight makes it imperative that any new security obligations be harmonized with other telecom-specific requirements.[7]

To harmonize new security assessment methodologies with existing regulation of the telecommunications industry, CTIA recommends a few revisions to the Interim Rule. First, DoD should recognize that, from a contracting perspective, telecommunications equipment and services are unique. Telecommunications providers offer the government access to robust commercial networks, which are regulated by federal and state agencies. DoD should clarify that such communications services are commercially available off-the-shelf ("COTS") items exempt from application of the CMMC and NIST SP 800-171 Assessment requirements.[8]

Second, the Department should address ambiguities in the Interim Rule that create the potential for divergent application across the government. These include the number and types

---

Department of Veterans Affairs (VA) to help make telehealth services more accessible to veterans," making T-Mobile the primary wireless provider for the VA. Press Release, T-Mobile, U.S. Department of Veterans Affairs Partners with T-Mobile to Help Expand Access to Health Care for Veterans (Dec. 10, 2018), https://www.t-mobile.com/news/va-veteranshealth-administration?icid=B2B_BB_19TFBEVRGN_XDYWUSXP417H9TQZO16875 .

[7] For example, the U.S. Navy's September 28, 2018, memorandum entitled, "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks" requires certain contractors to allow NCIS to "install network sensors, owned and maintained by NCIS, on the contractor's information systems . . . ." It is unclear what this requirement will look like in practice, but it would seem to be inconsistent with carriers' obligations under the Stored Communications Act and the Wiretap Act to not disclose communications to the government without proper legal process. *See* Memorandum from the Assistant Sec. of the Navy on Implementation of Enhanced Sec. Controls on Select Defense Industrial Base Partner Networks (Sept. 28, 2020), http://thecgp.org/images/ASN-SIGNED-IMPLEMENTATION-OF-ENHANCED-SECURITY-CONTROL.pdf.

[8] *See*, *e.g.*, 48 C.F.R. § 252.

of information systems for which a NIST SP 800-171 assessment must be performed, as well as whether contracts will be modified mid-performance to require a certain CMMC Level.

Finally, DoD should take a more realistic approach to the burden associated with implementation of these new processes. DoD should provide industry more time to engage with the government on substantive issues, particularly with respect to CMMC, where roll out will span the next five years and is likely to have significant direct and indirect effects.

II. CTIA'S MEMBERS SUPPORT THE FEDERAL GOVERNMENT'S MISSION TO PROTECT INFORMATION SYSTEMS.

CTIA and its members have a well-established track record of working with the government on cybersecurity and supply chain security, including with NIST and DoD on the development of the two assessment components of the Interim Rule. CTIA provided comments on the draft NIST SP 800-171B,[9] and regularly works with NIST and the Department on cybersecurity and supply chain matters.

CTIA has taken an active role in promoting cybersecurity and supply chain risk management across the federal government. Most recently, CTIA commented on the Federal Acquisition Security Council's ("FASC") Interim Final Rule and Request for Comments on the operations of the FASC, the sharing of risk information, and removal and exclusion orders.[10] CTIA also commented on DoD's Request for Information ("RFI") regarding Dynamic Spectrum Sharing, addressing issues at the intersection of telecommunications, national security, homeland security, and privacy.[11] CTIA joined other communications trade associations to advise the FAR Council on its interim final rule implementing Part B of Section 889 of the FY2019 National

[9] Comments of CTIA on Draft NIST SP 800-171B (filed Aug. 2, 2019).

[10] Comments of CTIA on Interim Final Rule with Request for Comments, 85 Fed. Reg. 54263 (filed Nov. 2, 2020).

[11] Comments of CTIA on Request for Information Regarding Spectrum Sharing, Department of Defense RFI (filed Oct. 19, 2020).

Defense Authorization Act.[12] Specifically, how the lack of clarity in the statute and rule had implications for commercial entities providing telecommunications services to the federal government merits action. The communications industry has helped agencies implement the *Secure Networks Act*,[13] as well as Executive Order 13873.[14] CTIA and its members have been active in FCC, National Telecommunications Information Administration ("NTIA"), and Department of Commerce proceedings to implement the Act.[15]

CTIA and its members are engaged in public-private partnerships to improve the cybersecurity of government and the private sector. They work with the Department of Homeland Security's ICT Supply Chain Risk Management ("SCRM") Task Force,[16] the Communications Sector Coordinating Council ("CSCC"),[17] the FCC's Communications Security, Reliability and Interoperability Council ("CSRIC"),[18] the Alliance for

---

[12] Comments of CTIA, NCTA, and USTelecom, 85 Fed. Reg. 42665, FAR Case 2019-0009, RIN 9000-AN92 (filed Sept. 14, 2020) ("Joint Associations Comments").

[13] Secure and Trusted Communications Networks Act of 2019, Pub. L. 116-124, 133 Stat. 158 (2020) ("Secure Networks Act").

[14] Executive Order No. 13873, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 15, 2019).

[15] *See*, *e.g.*, Comments of CTIA, WC Docket No. 18-89 (filed Aug. 31, 2020); Comments of CTIA, WC Docket No. 18-89 (filed May 20, 2020); Comments of CTIA, Docket No. 200609-0154, RIN 0660-XC046 (filed Jul. 28, 2020); Comments of CTIA, Docket No. 200521–0144, RIN 0660-XC047 (filed Jun. 25, 2020).

[16] DHS's ICT SCRM Task Force is a public-private partnership that addresses cyber threats to ICT supply chains through a "collective defense approach." The ICT SCRM has four work streams that identify risks and develop processes for ensuring secure supply chains. *See id.*; *see also Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*, CISA, https://www.cisa.gov/ict-scrm-task-force (last visited Nov. 19, 2020).

[17] The CSCC was chartered in 2005 to help coordinate initiatives to improve the physical and cyber security of sector assets and to ease the flow of information within the sector, across sectors and with designated Federal agencies. *See About the CSCC*, CSCC (2018), https://www.comms-scc.org/about-1.

[18] The CSRIC is an advisory committee led by the private sector that makes recommendations to the FCC to promote the security, reliability, and resiliency of the U.S. communications systems. Last year, CSRIC produced a "Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks," which made recommendations for action on supply chain issues. *See Addendum to Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks*, CSRIC Working Group 3, at A-4, (Sept. 2018), https://www.fcc.gov/file/14855/download.

Telecommunications Industry Solutions ("ATIS") 5G Supply Chain Working Group,[19] and NTIA's multi-stakeholder process on Software Component Transparency,[20] to name a few.

The communications sector is a vital contributor to government functions and takes seriously the security and reliability of its services. CTIA and its members offer years of practical experience to help the FAR Council secure U.S. communications from national and economic security threats, consistent with the reality of modern communications infrastructure, and the need to maintain a robust marketplace for government contracts.

III. THE RULE SHOULD ACCOUNT FOR THE UNIQUE ROLE OF TELECOMMUNICATIONS AND DATA SERVICES IN GOVERNMENT CONTRACTS.

A. The FAR Council Should Clarify That Commercial Wireless Services Are COTS Items, and Contracts Are Exempt From the NIST SP 800-171 Assessment and CMMC Requirements.

Wireless telecommunications companies provide DoD and other agencies with commercial services, as prime contractors and as subcontractors or suppliers to larger procurements.[21] The Interim Rule, as drafted, creates potential for different agencies—or different contracting officers within the same agency—to vary their interpretation of telecommunications services as COTS and the general application of the assessment requirements to specific telecommunications services. To prevent disparate application of the Interim Rule, DoD should extend previous guidance that commercial common carrier and data services—such as those previously categorized as "Plain Old Telephone Service" ("POTS")—are not information systems that process controlled unclassified information ("CUI"), but rather

[19] *See ATIS' 5G Supply Chain Working Group*, ATIS, https://www.atis.org/initiatives/5g-supply-chain-working-group/ (last visited Nov. 19, 2020).

[20] *See NTIA Software Component Transparency*, NTIA (Oct. 19, 2020), https://www.ntia.doc.gov/SoftwareTransparency.

[21] *See supra* Section I.

systems presumed not to provide data protection unless separately encrypted.[22] In extending this guidance, DoD should expressly recognize that commercial wireless services are best treated as COTS and outside the scope of the Interim Rule.

Due to the inherently low risk of COTS items involving confidential defense information ("CDI"), the Interim Rule—as well as DoD guidance applicable to DFARS 252.204-7012—makes clear that in procurements "solely" for COTS products, contractors need not comply with the NIST SP 800-171 requirements[23] nor the CMMC regime. The question then, is whether a telecommunication service qualifies as a COTS item. The Interim Rule does not conduct a unique evaluation of specific products and services, but incorporates the FAR definition of a COTS item, which is defined as any "***item of supply*** . . . that is (i) a commercial item [as defined by the FAR]; (ii) [s]old in substantial quantities in the commercial marketplace; and (iii) [o]ffered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace."[24]

This definition properly could be understood to include services like POTS and commercial wireless services, which are commercially offered in substantial quantity and without substantial change to the government. Shortly after the release of the Interim Rule the

---

[22] DoD Procurement Toolbox, *Cybersecurity FAQs, rev3*, DoD (July 30, 2020), https://dodprocurementtoolbox.com/faqs/cybersecurity, at 65-66, Q103 ("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.").

[23] *Id.* at 18, Q6 ("DFARS clause 252.204-7012 does apply to contracts for commercial items, but not to contracts solely for the acquisition of commercial-of-the-shelf (COTS) items. If you are primarily selling commercial items and not modifying them for DoD (i.e., COTS), DFARS clause 252.204-7012 (even if included) and NIST SP 800-171 would not apply.").

[24] FAR 2.101 (emphasis added).

FAR Council released a proposed rule to amend the definition of "commercial item,"[25] suggesting that its actions would alter the definition of COTS as it applies in the Interim Rule. Under the FAR Council's proposal, "commercial item" would be split into two separate subcategories—"commercial products" and "commercial services"—with only the former qualifying as a COTS item.[26] The FAR Council further proposes to only include "commercial products" in the Section 12.103 definition of COTS items.[27] CTIA urges the FAR Council not to take a narrow approach and instead to clarify that commercial wireless telecom and data services can be treated as COTS. As an Advisory Panel report cited in that rulemaking observed, "[t]he flow down of government-unique terms and conditions represents a costly and administratively complex demand on contractors engaged in the sale of commercial products to the federal government."[28] This is particularly so because "variation in definitions for commercial items represent an oversight or drafting error, rather than a deliberate policy decision. This lack of definitional unity can carry real consequences, potentially generating confusion and risking disputes among stakeholders applying differing interpretations of commercial products and commercial services to the procurement process."[29]

CTIA urges DoD and the FAR Council to ensure that the definitions adopted herein are consistent across these parallel rulemakings and take particular cognizance of the status of commercial wireless voice and data services in federal procurement. DoD should recognize that

[25] Federal Acquisition Regulation: Revision of Definition of "Commercial Item," 85 Fed. Reg. 65610 (Oct. 15, 2020) ("Commercial Item Proposed Rule").

[26] *Id*.

[27] *Id*. at 48 C.F.R. § 12.103 (as proposed).

[28] Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations Vol. 1 of 3 (January 2018), https://discover.dtic.mil/wp-content/uploads/809-Panel-2019/Volume1/Sec809Panel_Vol1-Report_Jan2018.pdf.

[29] *Id.*

the definition on which it relies is in flux, and that this variability has wide-ranging implications for contractors subject to the Interim Rule. However, CTIA also encourages DoD to take this opportunity to clarify that commercial telecommunications services continue to qualify at COTS under the revised Section 12.203. Such services are sold in substantial quantities in the commercial marketplace and offered to the government without modification; they would have previously qualified as an "item of supply," and should continue to qualify under the revised Section 12.203. CTIA will concurrently encourage the FAR Council to amend the definition of "commercial item" to include "commercial products or commercial services" in order to alleviate any ambiguity.

B. Telecommunications Regulations Present Unique Issues in the Application of CMMC and DFARS 252.204-7012.

Telecommunications and data services carriers are unique contractors. Each carrier builds out and operates a network from which it offers services to a multitude of customers, most commonly beginning with the general public and commercial customers. In order to provide these services, commercial networks operate in compliance with federal and state regulatory requirements. Given that government customers benefit from their use of contractors' commercial networks, which first and foremost provide a commercial service, telecom contractors cannot be presumed to customize their information systems and networks to comply with conflicting or diverging government-specific requirements, particularly those that could put them in violation of customary industry practices or their operating authorizations.[30]

Telecommunications providers may face unique challenges implementing certain government expectations in their commercial networks. For example, to achieve CMMC Level

[30] *See* Joint Association Comments, *supra* n.12, at 12-14 (discussing the regulatory obligations such as interconnection and roaming).

4, a contractor must implement Network Segmentation. Commercial networks serve government, contractor, and commercial customers. Wireless carriers of course deploy core security principles of appropriate network segmentation but may approach segmentation in a fundamentally different manner than traditional government contractors who segment enterprise network functions and databases. For example, network slicing is an evolving technology that enables the operators to provide a secure virtual network slice or slices to support different customers (including government) and varied functions or services, from high speed mobile broadband to low latency (AR/VR applications) to massive IoT (logistics and warehousing use cases). This is a fundamental improvement in network management and security, that is unique to 5G. As an IEEE paper explains, network slicing "belongs to the category of virtualization networking paradigm, together with Software-Defined Networking (SDN) and Network Function Virtualization (NFV). Network slicing can take advantage of SDN and NFV, but it can be seen as an independent technology enables the flexible and efficient creation of specialized end-to-end logical networks on top of shared network infrastructure. Each of these logical networks is able to accommodate a specific type of services, with different and heterogeneous requirements that facilitate vertical industries."[31] This may not be the sort of network segmentation that CMMC auditors or contracting officers recognize, but it holds immense promise for commercial and government customers.

Government agencies rely on commercial networks to provide foundational yet essential federal contracts and programs. Access to these networks is critical for most agencies, domestically and abroad. It is imperative that commercial telecommunications operators be able

[31] R. Olimid, Gianfranco Nencioni, 5G Network Slicing: A Security Overview, IEEE, (May 2020), https://ieeexplore.ieee.org/document/9099823?denied=.

to participate in government procurement. Therefore, DoD should ensure that its Interim Rule does not limit or unduly burden the participation of private sector partners in the telecom sector.

IV. DOD SHOULD ADDRESS AMBIGUITIES IN THE INTERIM RULE TO AVOID DIVERGENT APPLICATION ACROSS THE FEDERAL GOVERNMENT.

A. The NIST SP 800-171 and CMMC Assessment Requirements Create the Potential for Divergent Application by Contracting Officers and Agencies.

There are significant implementation issues attendant to NIST SP 800-171 and CMMC, which may create confusion or inconsistency during application. As written, the Interim Rule permits Contracting Officers or acquisition officials in different agencies to reach varying conclusions about which contractor information systems must be subject to a NIST SP 800-171 Assessment or must be certified to a particular CMMC Level. Similarly, Contracting Officers may take different approaches to subcontractors performing similar work under different contracts. This is compounded by potentially different interpretations among Contracting Officers or acquisition officials within the same agency. Potentially divergent interpretations may dramatically increase cost and uncertainty for offerors and should be addressed prior to the adoption of a final rule.

DoD should be mindful that the determination to apply these assessments is not limited to DoD and its contracting bodies—several Civilian agencies are expected to adopt CMMC, or particular elements of it, increasing the potential for disparate interpretations across the government. The General Services Administration ("GSA"), for example, has demonstrated an eagerness to apply these methodologies going forward, including a recent announcement that the STARS III solicitation, a Governmentwide Acquisition Contract to purchase information

technology services from 8(a) prime contractors, may include CMMC or aspects thereof.[32] GSA also included a CMMC Pilot Clause in the ASTRO Solicitation, a Multiple-Award Indefinite Delivery Indefinite Quantity contract under which GSA will acquire services for various federal agencies (including DoD), providing contractors the "voluntary opportunity to participate in CMMC assessments of the prime and select members of the supply chain."[33] The ASTRO Solicitation seeks to have contractors that handle CUI perform a CMMC Level 3 assessment, and those who do not handle CUI must perform a CMMC Level 1 assessment, in order to "provide the Government and contractors with awareness of their cyber vulnerabilities."[34] As other civilian agencies follow suit, unpredictability will make it difficult for companies to assess their obligations. The Interim Rule should be revised to require consistent interpretation and application across evaluating bodies.

B. Ambiguities in NIST SP 800-171 Assessments Compound Confusion About the Existing DFARS-7012 Clause.

As CTIA has highlighted in comments,[35] the Interim Rule contains controls with potentially divergent implementations for NIST SP 800-171 assessments. DoD should clarify aspects of the implementation to ensure consistent application across the government, including:

How Will Assessments Be Used? The Interim Rule provides that completing a basic assessment will be a threshold eligibility determination in order to award a contract/task

---

[32] *See CMMC requirements show up in GSA's STARS III contract,* FedScoop (July 8, 2020), https://www.fedscoop.com/cmmc-requirements-federal-contract-stars-iii-gsa/.

[33] *See ASTRO Solicitation, Clause H.15*, SAM.gov (Aug. 24, 2020), https://beta.sam.gov/opp/d4490b8661794e51bb83ec589a540a74/view#attachments-links ("This procurement has been identified as a CMMC Pilot activity. This will not be a condition of award, but will be a voluntary opportunity to participate in CMMC assessments of the prime and select members of the supply chain.").

[34] *Id*.

[35] *See*, *e.g.*, *supra* n.9.

order/delivery order or exercise an option under an existing contract.[36] However, there are several ambiguities that should be clarified.

- It is unclear from the Interim Rule whether Defense Contract Management Agency audits will be considered. Additionally, the Interim Rule should clarify whether or not the results of such Assessments could be used for other purposes.
- Informal guidance has suggested that a Contracting Officer is not foreclosed from considering assessment scores as a competitive evaluation factor in the source selection process.[37] However, the Interim Rule is silent on this potential use and, importantly, the weight such a factor would be given.
- The Interim Rule does not address whether a Contracting Officer considering assessment scores as competitive evaluation scores should assign higher significance to Medium or High assessments (which do not rely solely on contractor self-assessment). Conversely, the Interim Rule also does not specify whether a contractor could be penalized or face enforcement actions if a score fell below a certain threshold.

The Department should confirm that assessments will only be used as an element of a contractor's "responsibility" determination and not as a competitive evaluation criterion. DoD also should clarify in which instances it will verify contractor assessments at the Medium or High level, and whether a contractor may proactively request to be assessed at these levels.

Which Information Systems Must Have Assessments? The Interim Rule does not provide guidance to identify which information systems must be subject to an assessment. The Interim Rule provides that an assessment must be conducted for "each covered contractor information system that is *relevant* to the offer, contract, task order, or delivery order."[38] It does

[36] IFR at 61505 ("CMMC is designed to provide increased assurance to the Department that a [Defense Industrial Base] contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.").

[37] Comments of John Ellis, Director, Software Division, DCMA-TDW, at *Understanding the new DFARS Interim Cyber Assessment and CMMC Rule Webinar* (Oct. 6, 2020) (noting that while there is no written guidance on using Assessment scores as competitive evaluation factors, he expects that project managers and contracting officers will be using the information to work with their contractors and instill some competition to increase the scores of low-scoring companies).

[38] IFR at 61505.

not, however, provide guidance on how to assess which information systems are "relevant." By failing to define key identifiers, the Interim Rule creates ambiguities that could bar otherwise qualified contractors. As written, if a contractor fails to conduct an assessment for an information system that is later deemed "relevant" by a Contracting Officer at the time of award, the contractor would be found to be ineligible.

This ambiguity may harm the government and its contractors. First, in the absence of guidance, contractors may need to conduct assessments on more information systems than would otherwise be necessary, in order to limit the risk of possible disqualification from a competition or the risk that a Contracting Officer declines to exercise a contract option. The costs and burdens associated with such assessments to ensure compliance were not taken into account in the Interim Rule.

Second, and relatedly, many contractors—especially small businesses—may consider the added cost and competitive uncertainty as incentives to exit, or disincentives to enter, the government contracts marketplace.[39] Contractors expect a degree of unpredictability about the manner in which proposals will be evaluated, but it is atypical for award eligibility to be conditioned on a subjective criterion which is ultimately at the discretion of a Contracting Officer. This may reduce competition and innovation in the government marketplace. In the telecommunications sector, this may limit the government's access to innovative services and networks.

[39] A recent article highlighted concerns of small companies surrounding the implementation NIST SP 800-171 and CMMC, noting that manufacturers have ranging risks tolerances, but not a lot of actual cybersecurity expertise at each company. The article states that CMMC leaves Manufacturing Extension Partnerships "perplexed and paralyzed," and they "don't know where to start," with NIST SP 800-171. Sara Friedman, *NIST-funded small business centers push back against Pentagon messaging on CMMC preparedness*, Inside Cybersecurity (Nov. 18, 2020), https://insidecybersecurity.com/daily-news/nist-funded-small-business-centers-push-back-against-pentagon-messaging-cmmc-preparedness?destination=node/11825.

How Will Assessments Apply to Contracts Containing DFARS 252.204-7012 When There is No CDI? The Interim Rule recognizes that many contractors perform under contracts that contain the DFARS 252.204-7012 clause but they "never [receive, process, store, or use] CDI . . . [and therefore] do not have to implement NIST SP 800-171."[40] However, the Interim Rule is silent as to whether such contractors will need to submit NIST SP 800-171 Assessments. DoD should clarify that these contractors—those who do not process CDI and do not implement NIST SP 800-171—do not need to submit assessments.

Additionally, contractors should be provided a way to make this assertion to the government at the offer stage, so that Contracting Officers are not able to question at the time of award whether a contractor has simply failed to comply with the requirement to submit an assessment. For similar reasons, it is critical that Contracting Officers clearly state in solicitations whether CDI will be processed or provided by the contractor.[41]

C. The CMMC Requirement Presents Ambiguities That Require Clarification.

The Interim Rule's implementation requirements for CMMC also contain ambiguities that should be addressed prior to the adoption of the final rule. DoD should clarify components of the implementation process to ensure consistent application across the government, including:

Possessing a CMMC Level at the Time of Award. The Interim Rule specifies that offerors must possess the required CMMC Level at the time of award. As CMMC is rolled out, it is likely that many offerors (or their subcontractors) will be waiting for the necessary CMMC Level to be issued (or appeals to be adjudicated) while proposals are pending. Delays in

[40] IFR at 61510.

[41] There are additional inconsistencies arising out of CMMC's development while other security standards were under revision. Most notably, CMMC Levels 4 and 5 require implementation of security controls developed under NIST SP 800-171B (Draft), which has since been superseded by NIST SP 800-172. To reduce confusion and inconsistencies, DoD should facilitate collaboration and coordination with the CMMC AB and NIST.

receiving CMMC Levels are to be expected during the initial years of the regime as demand for assessors will outpace the availability of assessors and Certified Third-Party Assessment Organizations ("C3PAOs"). DoD explicitly recognizes in the Interim Rule that it will likely take seven years to implement initial CMMC certifications across the existing DoD contractor population.[42]

Although the first class of several dozen CMMC provisional assessors has completed their training,[43] DoD estimates that it will need as many as 10,000 assessors working full time to perform the expected number of CMMC certifications in the initial certification rollout.[44] If the Interim Rule is read to require contractors to possess the requisite CMMC level prior to submitting an offer, the rule would result in inequities in which eligibility for award would be contingent on the availability of private assessors and the speed with those assessors can complete CMMC certifications—factors contractors cannot control or influence.

Compounding the arbitrary timing of obtaining certifications, the date and time of award is generally subject to an agency's broad discretion. As a result, an agency could reduce competition by accelerating its award schedule, thereby eliminating any offerors with pending CMMC certifications. This degree of unpredictability and arbitrariness could further discourage contractors, particularly small businesses with modest internal IT resources, from investing resources in pursuing federal contract opportunities. Telecommunications carriers and other

---

[42] IFR at 61511.

[43] *See* Sara Friedman, *Costs for CMMC compliance difficult to predict based on DOD rule, experts say*, Inside Cybersecurity (Nov. 18, 2020), https://insidecybersecurity.com/daily-news/costs-cmmc-compliance-difficult-predict-based-dod-rule-experts-say ("The CMMC Accreditation Body completed its second training for provisional assessors this week with 36 individuals participating. The assessors are part of a cohort of 72 individuals who were selected by the CMMC AB in August for training to become assessors.").

[44] *See* CMMC Accreditation Body, https://www.cmmcab.org/ (last visited Nov. 19, 2020); *see also* Frank Kendall, *Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May*, FORBES (Apr. 29, 2020), https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/?sh=490c82613bf2.

companies whose federal work comprises a small portion of its business, may consider whether to invest time and resources in pursuing government contracts if the process to qualify as eligible is perceived as arbitrary and outside the control of the contractor.

To prevent such an outcome, DoD should permit awards to offerors who, at the time of award, are undergoing a CMMC certification or are appealing a determination but can demonstrate that they have achieved a score of 110 on their Basic Assessment. Such representations would demonstrate that a contractor has met all security controls in NIST SP 800-171, necessarily providing that all practices in CMMC Level 1 would be satisfied, and that at least 110 out of 130 practices would be met for CMMC Level 3.[45] Such interim eligibility would give comfort to contractors that they could be eligible for award of contracts with CMMC Levels 1-3, even if their CMMC certification is not yet complete. At the same time, interim eligibility would mitigate risks to the government of an insufficient pool of offerors. The Department should also explicitly provide a timeline for any appeals to the CMMC Accreditation Body ("CMMC AB"), including providing a set number of days for the CMMC AB to make a preliminary assessment, and a shot clock for a final CMMC AB determination.

Indeed, part of the impetus for the Interim Rule was DoD's view that few contractors had implemented all required controls,[46] so contractors who are prepared to represent that they have met all NIST SP 800-171 controls should not be discouraged from competition simply because a CMMC certification is delayed.

---

[45] Patricia Toth, *NIST Handbook 162" NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, NIST (Nov. 2017), https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf.

[46] IFR at 61508 ("Findings from DoD Inspector General report . . . indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information.").

Maintaining a CMMC Level During Performance. The Interim Rule requires that contractors maintain a CMMC Level over the course of performance. However, without additional guidance, this requirement raises a number of practical questions, including: (1) what might cause a contractor to lose its CMMC Level or certification other than expiration of the certification at the end of the three-year term?; (2) if a contractor's CMMC Level expires or is downgraded during the course of performance, is the contractor required to notify DoD?; and (3) if a contractor's CMMC Level expires or is downgraded, can a contractor continue performance?

CTIA recommends that DoD clarify that the only way a CMMC Level can terminate is at the end of its three-year term, and that contractors can continue performing under a contract if there are any lapses in certification as a result of delays in the CMMC accreditation process. DoD should provide that the contractor's obligation is to timely initiate the accreditation renewal process within three years, and to continue that process in good faith. This will ensure that contractors have a single, transparent date against which they can plan and measure their compliance.

Modification of a Contract to Require a CMMC Level. The Interim Rule does not specify whether Contracting Officers are to modify existing contracts to include the new DFARS 252.204-7021 provision and require contractors to achieve CMMC compliance. CTIA recommends that DoD explain that existing contracts should not be modified to include this requirement, as contractors may not have had sufficient time to achieve certification during the course of performance. Moreover, for some contractors, compliance may be impracticable given the information systems used, and it would be unfair to impose such a requirement, especially without providing a mechanism to reimburse contractors for the costs of achieving compliance.

Application of CMMC Levels to Subcontracts and "Other Contractual Instruments." The Interim Rule provides that a contractor must include "the requirements of the [Interim Rule] in all applicable subcontracts or other contractual instruments."[47] The Interim Rule does not, however, define what vehicles fall within the scope of "other contractual instruments." DoD should clarify that contractors are only obligated to flow down CMMC Level requirements to their direct subcontractors—those between whom there is privity of contract and an oversight relationship. Furthermore, because private entities cannot access the Supplier Performance Risk System to validate the CMMC Levels of their subcontractors, DoD should clarify that prime contractors may rely on attestations by subcontractors about their achievement of the requisite CMMC Level and that prime contractors are not liable for any false statements made by subcontractors to that effect that were relied on by a prime contractor in good faith.

V. DOD SHOULD INCORPORATE REALISTIC TIME AND COST ESTIMATES FOR THE NEW CMMC PROGRAM.

The Interim Rule underestimates the costs of compliance, as well as the time and resources necessary for contractors to perform assessments and achieve CMMC certification. Although the CMMC AB has made progress, it has not yet stood up the resources to train assessors and establish a certification regime, particularly on the scale necessary to implement CMMC across the Defense Industrial Base. These delays suggest that the FAR Council should embrace a more realistic timeline and cost estimates.

The Federal government is not prepared to roll out these requirements, and certainly not on the scale or at the speed envisioned by the Interim Rule. As discussed, there are not enough assessors or C3PAO certified or in the pipeline to conduct the number of CMMC certifications

[47] IFR at 61506.

proposed.[48] This problem is exacerbated by the uncertainty surrounding which systems require an assessment, as the anticipated number of certifications set out in the Interim Rule likely underestimates the number of certifications that will be requested by offerors in order to ensure their eligibility for award.

Moreover, the Interim Rule operates on a baseline assumption that contractors will have already implemented all NIST SP 800-171 security controls.[49] The cost estimates contained in the Interim Rule depend on this assumption. Yet the inability of contractors to consistently implement these security controls is the reason cited by DoD for the urgent circumstances necessitating the release of the Interim Rule.[50] Because not all contractors may have fully implemented the standard for NIST SP 800-171, the Interim Rule cannot properly consider companies that fall below that standard when calculating allowable cost estimates for CMMC Levels 3-5.[51]

CMMC is a new requirement that will be rolled out over at least five years, and industry should be provided with opportunity to engage DoD on the implementation of the CMMC initiative, which will have a range of impact on contractors for years. In recognition of the significant time and resources needed to achieve compliance with DFARS 252.204-7012 and NIST SP 800-171, DoD previously issued guidance[52] that contractors not yet in compliance with the requirements of NIST SP 800-171 could meet their contractual obligations by establishing a

[48] *Supra* n.43.

[49] IFR at 61507.

[50] *See id.* at 61505, 61518.

[51] *Id.* at 61507.

[52] *See* DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented, , 83 Fed. Reg. 17807 (Apr. 24, 2018), https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08554.pdf.

System Security Plan that outlines the contractor's current state of compliance and identified compliance gaps, and by preparing a Plan of Actions and Milestones ("POAM") for completing the implementation in the future. DoD should adopt similar guidance for CMMC to permit contractors to develop POAMs for the first three years of the roll out period, thereby offering contractors a tool to work towards full compliance without breaching contractual obligations.

The Interim Rule assumes that assessing compliance with the NIST SP 800-171 security controls is little more than a ministerial function, which can be performed by a GS-11 equivalent employee, or even a GS-9 clerk. In practice, the compliance functions related to its implementation are complex and require a multi-disciplinary approach drawing on technical, contracts, legal, and executive personnel with significant experience and responsibility. The FAR Council should be more realistic in its view of the burdens associated with these obligations.

VI. CONCLUSION

DoD should revise the Interim Rule and approach any final decision in this proceeding with an emphasis on clarity, predictability, and uniform applicability across the federal government.

Respectfully submitted,

By: */s/ Melanie K. Tiano*

Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

November 30, 2020