Before the Department of Defense
Washington, D.C.

In the Matter of

Defense Acquisition Regulations System:	)	Notice of Proposed Rulemaking
Assessing Contractor Implementation of	)	DFARS Case 2019-D041
Cybersecurity Requirements	)	

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

David Valdez
Vice President, Privacy and Cybersecurity

Justin C. Perkins
Director, Cybersecurity and Policy

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

October 15, 2024

Table of Contents

I. INTRODUCTION AND SUMMARY

CTIA[1] is pleased to submit comments on the Department of Defense ("DOD" or "Department") proposed rule amending the Defense Federal Acquisition Regulation Supplement ("DFARS") to incorporate contractual requirements for the Cybersecurity Maturity Model Certification 2.0 ("CMMC") program ("Proposed Rule"),[2] which is being developed in parallel to DOD's separate proceeding for the substantive CMMC 2.0 requirements consisting of a December 2023 Notice of Proposed Rulemaking ("CMMC 2.0 Program NPRM") and the October 2024 final CMMC 2.0 Program rule ("Final CMMC 2.0 Program Rule").[3] The Proposed Rule proposes to amend Chapter 48 of the Code of Federal Regulations ("C.F.R") to provide DFARS standard clauses for contracting officers to implement the CMMC 2.0 Program in all solicitations and contracts and to reference the CMMC 2.0 Program.[4] Among other requirements, the Proposed Rule would instruct contracting officers to identify and include the CMMC Program level required for each solicitation or contract,[5] and require contractors to

[1] CTIA® (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 providers, device manufacturers, 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] *See* Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, Notice of Proposed Rulemaking, 89 Fed. Reg. 66327 (Aug. 15, 2024), https://www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of ("Proposed Rule").

[3] *See Cybersecurity Maturity Model Certification (CMMC) Program*, Notice of Proposed Rulemaking, 88 Fed. Reg. 89058 (Dec. 26, 2023), https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program ("CMMC 2.0 Program NPRM"); *Cybersecurity Maturity Model Certification Program*, Final Rule, 89 Fed. Reg. 83092, (Oct. 15, 2024), https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program ("CMMC 2.0 Program Final Rule"). The Final CMMC 2.0 Program Rule was published in the Federal Register on the day of this filing, October 15, 2024.

[4] Proposed Rule at 66327.

[5] *Id*. at 66337, Proposed DFARS 252.204-7503(a).

provide affirmations of compliance with substantive security requirements before receiving a contract award, task order, or delivery order.[6]

CTIA has been engaged in the development of the CMMC Program and related proceedings since the program's inception,[7] given the wireless industry's unique role in contracting. Indeed, many CTIA members service government customers by offering telecommunications services over commercial networks, ranging from commercial wireless connectivity and devices to bespoke services for specific agency missions. And CTIA members also participate in DOD procurement as subcontractors on numerous contracts, providing connectivity and other communications solutions to prime contractors across multiple agencies.[8]

Based on the wireless industry's perspective, CTIA is pleased to continue to offer comments to DOD as it considers the practical implications of the CMMC 2.0 program on various contractors. Specifically, with these comments, CTIA:

> (1) urges DOD to clarify the scope of the CMMC Program to account for the role of telecommunications providers and to promote consistency with other Federal privacy and security regulatory regimes;
>
> (2) cautions DOD to avoid making changes to the requirements of the CMMC 2.0 Program through the implementing provisions of this Proposed Rule, and, to this end, encourages DOD to ensure that the draft DFARS clauses and provisions apply CMMC requirements only to data covered by the CMMC 2.0 Program's requirements and to

---

[6] *Id*., Proposed DFARS 252.204-7503(b).

[7] Comments of CTIA, Cybersecurity Maturity Model (CMMC), Draft CMMC v0.4 (filed Sept. 25, 2019); Comments of CTIA, Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, (filed Nov. 30, 2020), https://www.regulations.gov/comment/DARS-2020-0034-0125; Comments of CTIA, CMMC 2.0 Program Proposed Rule, (filed Feb. 26, 2024), https://www.regulations.gov/comment/DOD-2023-OS-0063-0317, ("CTIA CMMC 2.0 Program Comments"); Comments of CTIA, NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Initial Public Draft (filed July 14, 2023), https://csrc.nist.gov/csrc/media/projects/protecting-controlled-unclassified-information/Call-for-comments-July-2023/CUI_Call_CTIA_July17_2023.pdf.

[8] U.S. Dept. of the Navy, *Solicitation No. N0024-24-R-0003* (issued Jan. 30, 2024), available at https://sam.gov/opp/3e37d759ae294d7bacbe2cd1cfa5dca0/view; U.S. Dept. of the Air Force, *Solicitation No. FA872624RB015* (issued Mar. 22, 2024), available at https://sam.gov/opp/6c6dad8fceee46658b53630b499a552e/view.

refrain from adding a new set of cybersecurity incident reporting requirements that are not consistent with existing or proposed DFARS requirements; and

(3) encourages DOD to account for operational realities of implementing the CMMC 2.0 Program by clarifying that contractors may use multiple system enclaves or boundaries, and by providing clear guidance on the adoption of DOD unique identifiers.

II. DOD SHOULD ENSURE THAT THE CMMC 2.0 PROGRAM IS PROPERLY SCOPED TO ADDRESS UNIQUE ASPECTS OF TELECOMMUNICATIONS SERVICES AND TO ACCOUNT FOR DE-IDENTIFIED DATA.

A. DOD Should Clarify and Finalize the Exception for Telecommunications Providers, Given the Unique Role that They Play in the Contracting Ecosystem.

CTIA is pleased to see DOD recognize wireless companies' functions and contributions in DoD contracting, including in the current Proposed Rule as well as in the CMMC 2.0 Program NPRM and Final CMMC 2.0 Program Rule. Specifically, in the December 2023 CMMC 2.0 Program NPRM, DOD sought to clarify that CMMC level requirements would not apply to telecommunications service providers "unless those entities themselves are or intend to become defense contractors or subcontractors," and that commercial telecommunications or cloud carrier services are not within the CMMC Assessment Scope "as long as CUI is encrypted during transport" across those systems.[9] In this Proposed Rule, DOD helpfully clarifies the scope of CMMC requirements, explaining that "plain old telephone service" and "common carrier telecommunications systems" are not considered part of a covered contractor information system that processes Federal Contract Information ("FCI") or Controlled Unclassified Information ("CUI").[10] DOD further explains, and CTIA concurs, that even when contracts with telecommunications providers do include DFARS clause 252.204-7012, Safeguarding Covered

[9] CMCC 2.0 Program NPRM at 89067. In its February 2024 comments on the CMMC 2.0 Program NPRM, CTIA recommended that DOD clarify the intended exception for commercial telecommunications services from CMMC level requirements and Assessment Scope and proposed revisions to definitional provisions of 32 C.F.R Part 170. CTIA CMMC 2.0 Program Comments at 3-5.

[10] Proposed Rule at 66331.

Defense Information and Cyber Incident Reporting, the clause should not be interpreted to extend those requirements to the commercial telecommunications networks of the provider.[11] Finally, in the Final CMMC 2.0 Program Rule, DOD rightly explains that a telecommunications provider's information system is not within a contractor's CMMC Assessment Scope if the CUI transiting that system is properly encrypted during transport.[12] DOD further clarifies that it is the Organization Seeking Assessment ("OSA") (*i.e.,* the contractor), not the telecommunications network provider, which is responsible for encrypting the CUI.[13]

While the recognition of an exception for commercial telecommunications services detailed above is a step in the right direction, DOD should provide further clarification. *First,* as CTIA has previously explained, use of the term "common carrier" is a defined term of federal law that could be overly restrictive if used in this context.[14] While DOD has indicated that its use of the term "common carrier" is derived from another document outside the scope of the CMMC Program,[15] DOD should nevertheless make clear that there is an exception for contracts involving commercial communications networks that support government and commercial traffic, and which are not purpose-built for use by the federal government to transmit sensitive or other government data, regardless of an entity's designation as a "common carrier." To ensure that DOD's exception for commercial telecommunications networks is clear, CTIA reiterates its

[11] *Id*.

[12] CMMC 2.0 Program Final Rule at 83113.

[13] *Id*. (stating that a "lack of adequate encryption on the part of the OSA would not trigger application of CMMC requirements" to the telecommunications provider's network).

[14] CTIA CMMC 2.0 Program Comments at 3-4.

[15] CMMC 2.0 Program Final Rule at 83113 ("The term 'common carrier' appears in the comment section to a previous rule making process. Its definition and use are taken from CNSSI 4009. Efforts to define it or related terms by other agencies are outside the scope of the CMMC Program.")

previously proposed language that DOD should add to address this issue.[16] Specifically, DOD should add a definition of "contractor information system" to the Proposed Rule and define that term to mean:

> "an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information, CUI, or FCI. It does not include commercial communications networks that transmit government and non-government information using the same equipment, protocols, and methodologies, without regard to the source or recipient of the information."

Second, DOD should continue to clarify—as it has done in the Final CMMC 2.0 Program Rule—that the responsibility for compliance with any encryption requirements for FCI or CUI data being sent over commercial communications networks belongs to the contracting agency or (as applicable) the prime contractor—not the telecommunications provider. While the Final CMMC 2.0 Program Rule includes a helpful discussion on this issue, as detailed above, unfortunately, the current Proposed Rule still introduces ambiguity.[17] As CTIA has urged in past advocacy,[18] the responsibility for this encryption should clearly lie with the relevant contracting agency customer or prime contractor. Telecommunications providers cannot encrypt traffic on behalf of their customers in this context and should not be faced with apparent risk of being subject to CMMC requirements and potential accountability because of a failure by their customer, whether government agency or prime contractor, to comply with the customer's obligations. DOD should ensure that this is clear in *both* the CMMC 2.0 Program Rule *and* under the current Proposed Rule.

---

[16] CTIA CMMC 2.0 Program Comments at 4-5.

[17] DOD notes that "[d]ata traversing common carrier systems should be separately encrypted per NIST SP 800–171 requirement 3.13.8." Proposed Rule at 66331. This is ambiguous and may create uncertainty and compliance challenges.

[18] CTIA CMMC 2.0 Program Comments at 3.

Making these changes to the Proposed Rule would have significant benefits for both DOD and telecommunications providers by reducing confusion, clearly allocating responsibility for implementing encryption controls for protected data, and reducing unnecessary implementation and compliance costs for commercial telecommunications services. With the recent release of the Final CMMC 2.0 Program Rule, it is even more crucial that DOD ensure that the two proceedings establishing this program are giving consistent and clear guidance.

B. DOD Should Establish an Exemption from CMMC Requirements for De-Identified Data, Consistent with Longstanding Approaches to Privacy and Security.

In addition to clarifying an exception for commercial telecommunications services, DOD should further focus the CMMC 2.0 Program on high-risk data by creating an exemption for de-identified data from the definition of CUI in this proceeding,[19] which would relieve contractors that process, store, or transmit de-identified data from CMMC 2.0 Program compliance for such data.[20]

An exemption for de-identified data would be consistent with baseline privacy and security principles already established by Federal agencies. The Department of Health and Human Services' ("HHS") Health Insurance Portability and Accountability Act ("HIPAA") is a prime example of a longstanding federal framework intended to protect sensitive data that exempts de-identified information. In particular, privacy regulation under HIPAA exempts from requirements information "that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual."[21]

---

[19] *See* Proposed Rule at 66336; Proposed DFARS 252.204-7501 (defining CUI).

[20] *See* Proposed Rule at 66330, 66338; Proposed DFARS 252.204-7021(a). While DOD can implement this exception as to the definition of CUI that applies to the CMMC Program, DOD should also work with the National Archives and Records Administration and other relevant Federal agencies to implement this definition uniformly across the government.

[21] 45 C.F.R. §164.514(a). HHS has also provided detailed guidance for regulated entities on how to take advantage

Similarly, the Federal Trade Commission ("FTC") has long held that its consumer data guidance does not apply to de-identified data, provided that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.[22] The Federal Communications Commission's ("FCC") privacy regulations on personal information are limited to "personally identifiable information,"[23] while use restrictions on customer proprietary network information ("CPNI") apply only to "individually identifiable CPNI."[24]

Exempting de-identified information from the definition of CUI would have significant benefits for DOD because doing so would enable the Department to focus its protection efforts on the most sensitive CUI and FCI, and associated assets. Likewise, such an approach would benefit defense industrial base firms by allowing them to prioritize their protection and compliance efforts on truly sensitive data and the systems that process, store, or transmit such data. In addition to modifying the definition of CUI in this proceeding, DOD should work with relevant agencies, including the National Archives and Records Administration, to implement a de-identified data exception for all Federal CUI regulations.

---

of this exception. HHS, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[22] FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at iv, (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[23] *Data Breach Reporting Requirements*, Report and Order, 89 Fed. Reg. 9968, 10003 (Feb. 12, 2024), Proposed 47 C.F.R. § 64.2011(c)(5).

[24] *See* 47 C.F.R. § 64.2007(b).

III. DOD'S DRAFT DFARS CLAUSES AND PROVISIONS SHOULD BE UPDATED TO MIRROR THE SCOPE AND SUBSTANCE OF THE CMMC 2.0 PROGRAM REQUIREMENTS.

Overall, any new DFARS clauses and provisions that are adopted to implement the CMMC 2.0 Program should not stray from the substantive CMMC 2.0 Program requirements, which were finalized under a separate rulemaking process on October 15, 2024.[25] Unfortunately, however, the Proposed Rule as drafted provides implementing instructions and procedures for contracting officers to execute the CMMC 2.0 Program that are out of sync with the CMMC 2.0 Program requirements, as detailed below. Therefore, DOD should revise and focus the Proposed Rule to ensure that the new provisions and clauses do not make substantive changes or add new requirements to the CMMC 2.0 Program.

A. DFARS Clauses and Provisions Implementing CMMC Requirements Should Only Apply to Data Covered by the CMMC 2.0 Program.

The CMMC 2.0 Program will require DOD contractors to implement prescribed cybersecurity standards to safeguard FCI and CUI, as well as to conduct assessments of contractor information systems that process, store, or transmit FCI or CUI and to prepare certifications regarding those assessments for submission to the government.[26] To implement these program requirements, DOD has here proposed a contract clause that would require contractors to use only information systems that have an appropriate CMMC certification in performing the subject contract.[27]

---

[25] CMMC 2.0 Program Final Rule, 89 Fed. Reg. 83092.

[26] CMMC 2.0 Program NPRM at 89118, Proposed 32 C.F.R. §170.1. *See also* CMMC 2.0 Program Final Rule at 83174 ("[t]he CMMC Program couples an affirmation of compliance with certification assessment requirements to verify OSA implementation of cybersecurity requirements.").

[27] Proposed Rule at 66338, Proposed DFARS 252.204-7021(b)(3).

This proposed contract clause is overly broad. It is not limited to specific types of information covered by the CMMC 2.0 Program (*i.e.,* FCI and CUI) or information that is not yet encrypted for external transmission (as NIST 800-171, Rev. 2, Requirement 3.13.8 contemplates).[28] The Proposed Rule makes no distinction for what types of information systems are capable of being certified under the CMMC Program. Instead, the draft DFARS provisions appear to apply to processing, storing, or transmitting "data." As such, it could be read to establish requirements for all of a contractor's data processing, instead of limiting requirements to specific types of information covered by existing DFARS requirements or by CMMC 2.0, and could be read not to allow contractors to "process, store, or transmit data" of any type on information systems owned or operated by entities that are not subject to CMMC 2.0. As drafted, the Proposed Rule goes far beyond the intended scope of the CMMC 2.0 Program, and would impose massive costs on contractors, who would have to implement and assess controls intended for FCI and CUI on all of their information systems.

To ensure that the implementation of the CMMC 2.0 Program remains consistent with its intended scope, DOD should revise the draft clause at 252.204-7021(b) as follows:

> (b) *Requirements*. The Contractor shall—
>
> (3) Only process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) data used in performance of the contract on information systems that have a CMMC certificate or CMMC self-assessment at the CMMC level required by the contract, or higher[.][29]

[28] NIST SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST, at 38 (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf ("3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.").

[29] Note that proposed additions are marked in blue font.

B. DOD Should Not Require an Additional, Supplemental Report of "Lapses" to Contracting Officers.

The Proposed Rule seeks to introduce a new requirement that contractors report to Contracting Officers "within 72 hours when there are any lapses in information security . . . during [the] performance of a contract."[30] This proposal is problematic from both an operational and policy perspective.

First, it is unclear what might be considered a reportable lapse. The term "lapse" is not defined—and it is not widely used in the normal lexicon of cyber incident reporting. Accordingly, contractors will have significant challenges in determining whether an event must be reported to a contracting officer under this proposal. Moreover, the draft DFARS provision could be interpreted quite broadly, as it does not clearly limit reportable "lapses" to only those affecting covered information systems or the CUI or FCI residing on those systems. This imprecision is highly problematic.

Second, the draft DFARS provision could be read to effectively add a substantive incident reporting requirement, distinct from the other substantive requirements for the CMMC 2.0 Program. Adding new requirements at this stage of the proceeding raises procedural issues and is inconsistent with the CMMC 2.0 Program Final Rule.[31] This new reporting obligation also goes beyond the stated goals of the DoD with this Proposed Rule,[32] and DoD should not use

[30] Proposed Rule at 66338, Proposed DFARS 252.204-7021(b)(4).

[31] Indeed, DOD has acknowledged in the CMMC 2.0 Program Final Rule that the assessment framework is not intended to add or modify cyber incident reporting requirements. CMMC 2.0 Program Final Rule at 83108 ("This rule contains no cyber incident reporting requirements.").

[32] Proposed Rule at 66327 ("The proposed changes to the existing DFARS language are primarily to: (1) add references to the CMMC 2.0 program requirements proposed at 32 C.F.R. part 170; (2) add definitions for controlled unclassified information (CUI) and DoD unique identifier (DoD UID) to the subpart; (3) establish a solicitation provision and prescription; and (4) revise the existing clause language and prescription.").

these draft contract clauses and provisions to impose new substantive CMMC Program requirements.

Third, the introduction of a new reporting requirement raises serious policy concerns because the Proposed Rule creates tension with the many already existing incident reporting requirements, including DFARS 252.204-7012.[33] For example, DOD here proposes new and distinct requirements for reporting to contracting officers, when similar reports are already required through the Defense Industrial Base Cybersecurity Portal ("DIB Portal").[34] The Proposed Rule also uses a different definition of what must be reported to a contracting officer, and a different timeline of when reports must be made, when compared to existing cyber incident reporting requirements. The Proposed Rule is also not consistent with proposed modifications in yet another separate Federal Acquisition Regulatory Council proceeding that would require reporting of cybersecurity incidents to both a government-provided portal and to the contracting officer.[35] Accordingly, the Proposed Rule is in tension with the goal of harmonizing federal cybersecurity and incident reporting requirements, which is shared by both the White House[36]

[33] DFARS 252.204-7012(c).

[34] DOD, Defense Industrial Base Cybersecurity Portal (last accessed Oct. 10, 2024), https://dibnet.dod.mil/dibnet/.

[35] *See Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing*, Notice of Proposed Rulemaking, 88 Fed. Reg. 68055, 68059 (Oct. 3, 2023), https://www.govinfo.gov/content/pkg/FR-2023-10-03/pdf/2023-21328.pdf.

[36] It is the stated policy of the Administration to support the harmonization of federal agencies' cybersecurity regulatory requirements. The White House, National Cybersecurity Strategy, at 9 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf ("Where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms"); The White House, National Cybersecurity Strategy Implementation Plan, at 12 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (assigning the Office of the National Cyber Director to "identify opportunities to harmonize cybersecurity baseline requirements for critical infrastructure").

and DOD,[37] and DOD has already explained in the CMMC 2.0 Program Final Rule that the program is not intended to change contractors' cybersecurity incident reporting requirements.[38]

In fact, instead of promoting harmonization, this Proposed Rule would add to the already complex patchwork of incident reporting requirements that government contractors have to navigate, even beyond DOD and Federal Acquisition Regulation contracting requirements. As the Department of Homeland Security's ("DHS") Cyber Incident Reporting Council found in its report, there are 52 in-effect or proposed reporting requirements to 22 agencies—and that is just at the federal level.[39] For example, telecommunications providers that are also government contractors will be subject to the incident reporting rules being created under the Cyber Incident Reporting for Critical Infrastructure Act of 2022,[40] and have obligations to the FCC to report breaches of customer data.[41] The Office of Management and Budget has also recently required agencies to impose reporting requirements for contractors to notify agencies of "serious [Artificial Intelligence] incidents and malfunctions" within 72 hours.[42]

---

[37] DOD's own strategy for defense industrial base cybersecurity recognizes the importance of a collaborative approach that does not "introduce[e] undue costs or burdens." DOD, Defense Industrial Base Cybersecurity Strategy 2024, at 25 (Mar. 21, 2024), https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF.

[38] CMMC Program 2.0 Final Rule at 83108 ("The CMMC assessment framework will not alter, alleviate, or replace the cyber incident reporting aspects of DFARS clause 252.204-7012[.]").

[39] DHS, Harmonization of Cyber Incident Reporting to the Federal Government, at 9, (2023), https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf. The Cyber Incident Reporting Council was created by statute in the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Homeland Security Act of 2002 § 2246, 6 U.S.C. § 681f (as added by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103, div. Y, § 103, 136 Stat. 49, 1054, (2022)).

[40] *See* CISA, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Notice of Proposed Rulemaking, 89 Fed. Reg. 23644 (Apr. 4, 2024), https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

[41] *See Data Breach Reporting Requirements*, Final Rule, 89 Fed. Reg. 9968 (Feb, 12, 2024), https://www.federalregister.gov/documents/2024/02/12/2024-01667/data-breach-reporting-requirements.

[42] Office of Management and Budget, Memorandum M-24-18: Advancing the Responsible Acquisition of Artificial Intelligence in Government, at 17 (Sept. 24, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/10/M-24-

Overall, adding this significant new incident reporting requirement through the DFARS contract clauses and provisions for the CMMC Program will result in several unintended consequences. Such a significant change to DOD's incident reporting requirements would burden contractors with confusing and inconsistent obligations, and create unnecessary and duplicative reporting, particularly for large contractors who engage with multiple contracting officers across various federal government contracts. Further exacerbating the impact of this proposal, many companies are likely to serve as subcontractors on numerous contracts, and would face obligations to report such events to their prime contractors where flowed down through subcontracts.[43]

For all of these reasons, DOD should not create "lapse" as a new category of reportable incident. Instead, it should reference existing incident reporting requirements, triggers, and incident definitions in the DFARS 252.204-7012, rather than creating new requirements or terms. DOD should also revise the Proposed Rule so that contracting officers receive reporting of qualifying cyber incidents directly from the DIB Portal. Contractors would then need to make only a single report of a cyber incident to DOD, rather than a separate, duplicative report to contracting officers.

C. DOD Should Clarify What "Changes" in CMMC Status a Contractor Must Report to a Contracting Officer.

In the current Proposed Rule, DOD has proposed that contractors must notify the contracting officer within 72 hours of "changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract."[44] As drafted, this language needs

18-AI-Acquisition-Memorandum.pdf.

[43] Proposed Rule at 66338, Proposed DFARS 252.204-7021(d)(1).

[44] *Id*. at 66338, Proposed DFARS 252.204-7021(b)(4).

clarification to avoid confusion and overreporting, which would be inconsistent with the Final CMMC 2.0 Program Rule.

First, DOD should clarify what type of "changes" will require notification to a contracting officer—and in doing so should focus on those that have material impacts, such as a recertification, renewal of a self-assessment, or a change in certification level. As such, the definition of "current" proposed in 252.204-7021(a) should be amended to include the term "material," for example:

> *Current* means, with regard to Cybersecurity Maturity Model Certification (CMMC)—(1) Not older than 1 year for Level 1 self- assessments, with no material changes in CMMC compliance since the date of the assessment[.]

Second, the Proposed Rule's explanatory material does not match what the draft DFARS clauses and provisions say about changes to CUI systems. DOD summarizes the draft changes to the clause at DFARS 252.204-7021 as requiring "the contractor to notify the contracting officer of any changes in the contractor information systems that process, store, or transmit FCI or CUI during contract performance. . . ."[45] Without clarification, the NPRM as drafted appears to require reporting to contracting officers of routine events, such as system maintenance or version updates. This is inconsistent with the text of the draft DFARS clause, which specifies that contracts must "[r]eport to the Contracting Officer any changes *to the list of DoD UIDs* applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract."[46]

DOD should not guide contractors to report "any changes" in contractor information systems,[47] and should instead clarify that such reporting is limited to when the contractor

[45] *Id*. at 66329.

[46] *Id*. at 66338, Proposed DFARS 252.204-7021(c)(3) (emphasis added).

[47] *Id*. at 66329.

changes the systems that are supporting the contract—not changes to the underlying systems themselves.

IV. DOD SHOULD ACCOUNT FOR OPERATIONAL REALITIES OF CMMC IMPLEMENTATION.

The Proposed Rule introduces significant new assessment and affirmation requirements on DOD contractors, and in doing so DOD should make every effort to provide clear guidance that does not unnecessarily disrupt existing contractor practices and expectations. In particular, DOD should ensure that its new rules permit multiple system enclaves in the performance of a contract, and DOD should provide training and guidance on the use of the CMMC 2.0 Program's unique identifier.

A. The DFARS Should Allow for Contractors to Use Multiple Information System Enclaves in the Performance of a Contract.

The draft DFARS solicitation provision at 252.204-7YYY(b)(1) seems to depart from DOD's previous policy statements to permit the use of multiple enclaves under the CMMC.[48] The proposed solicitation provision contemplates that the single certification or self-assessment level identified by the contracting officer will apply "for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during the performance of the contract."[49] The proposed provision therefore appears designed to allow contracting officers to identify the CMMC certification or self-assessment level required for a given contract.

Mandating a single assessment level for each contractor information system that processes, stores, or transmits FCI or CUI during the performance of the contract could

[48] *Id*. at 66338, Proposed DFARS 252.204-7YYY(b)(1).

[49] *Id*.

needlessly restrict how contractors structure their information systems. For example, it appears not to permit contractors to establish separate information systems that are structured to comply with different CMMC level requirements, such as one for handling FCI, another for handling CUI, and potentially even another for handling CUI of the type requiring Level 3 protection. As drafted, the proposed DFARS provisions could be read to require all contractor information systems processing, storing, or transmitting FCI or CUI during the performance of the contract to meet the *highest* CMMC level identified by the contracting officer. Requiring all contractor information systems processing, storing, or transmitting FCI or CUI during the performance of the contract to meet the highest CMMC level identified by the contracting officer, however, would preclude contractors from creating separate system enclaves by level and segregating the specific FCI or CUI that requires the given level of protection.

This is inconsistent with previous DOD statements in the CMMC 2.0 Program rulemaking, which noted the possibility that "different enclaves [might be] expected to process, store, or transmit information that needs different levels of security" in certain contracts,[50] and confirmed that "it is possible to have different business segments or different enclaves assessed or certified at different CMMC Levels."[51] Indeed, DOD states elsewhere in the current Proposed Rule that it expects contractors to have, "on average 5 contractor information systems that will be used to process, store, or transmit FCI or CUI in performance of the contract."[52] Requiring all contractor information systems processing, storing, or transmitting FCI or CUI during the

[50] CMMC 2.0 Program NPRM at 89074. *See also id.* at 89078 ("Defense contractors can achieve a specific CMMC Level for its entire enterprise network or an enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.").

[51] *Id*. at 89071. *See also* CMMC 2.0 Program Final Rule at 83202 ("[T]he Department does not intend to formulate specific directives pertaining to the configuration and segregation of corporate information systems into enclaves.").

[52] Proposed Rule at 66334.

performance of the contract to meet the highest CMMC level designated by the contracting officer, in turn, could necessitate far wider adoption of the CMMC Level 3 requirement than DOD predicted in the Program NPRM,[53] significantly raising compliance costs for industry and demand for qualified assessors. DOD should reframe the proposed DFARS provisions to clearly permit this multi-enclave approach.

B. DOD Should Provide Clear Guidance and Training on Use of the Unique Identifier Well in Advance of the Effective Date of the Program.

To reduce confusion and administrative burden on DOD contractors, DOD and the accreditation body Cyber AB should further support the introduction of the DOD unique identifier[54] with clear guidance that describes how to use the Supplier Performance Risk System.[55] Such guidance and training should be issued well in advance of the effective date of the CMMC 2.0 Program. This simple, practical step will ensure that contractors are prepared to implement new requirements and will limit unnecessary administrative burdens on DOD, assessors, and contractors.

V. CONCLUSION

CTIA applauds DOD for acknowledging the wireless communications industry's unique functions and contributions in the Department's response to comments on the application of CMMC requirements to telecommunications service providers. CTIA encourages DOD to clarify and formally adopt the exception for telecommunications providers in the Proposed Rule.

---

[53] CMMC Program NPRM at 89097-98 (estimating the number of entities annually conducting certification and affirmation at Level 3).

[54] Proposed Rule at 66338, Proposed DFARS 252.204-7021(a) ("*DoD unique identifier* means an alpha-numeric string of ten characters assigned within the Supplier Performance Risk System to each contractor assessment, with the first two characters indicating the confidence level of the assessment.") (emphasis in original).

[55] *See* Defense Information Systems Agency, "SPRS Supplier Performance Risk System Overview," https://www.sprs.csd.disa.mil/pdf/training/SPRS_Overview_Training-Presentation.pdf (noting that CMMC functionality is "coming").

In addition, CTIA recommends that DOD promote harmonization by 1) adopting an exception for de-identified data from the definition of CUI; and 2) ensuring that the Proposed Rule does not add new substantive requirements to the CMMC 2.0 Program. Specifically, DOD should remove proposed requirements for notification to contracting officers of "lapses" in information security that are inconsistent with current and proposed DOD incident reporting requirements for contractors, and clarify draft provisions in the Proposed Rule so as not to inadvertently apply CMMC to requirements to all contractor data systems—not just those that process, store, or transmit CUI or FCI in the performance of the contract. CTIA further recommends that DOD make revisions to the Proposed Rule to limit the changes in CMMC self-assessment levels that must be reported to contracting officers, consistent with the intent expressed in the Proposed Rule's explanatory material. Finally, DOD should take steps to limit unnecessary administrative burdens by explicitly permitting the use of multiple enclaves and providing clear guidance on the use of the new DOD unique identifier.

Respectfully,

/s/ Thomas K. Sawanobori
Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

David Valdez
Vice President, Privacy and Cybersecurity

Justin C. Perkins
Director, Cybersecurity and Policy

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

October 15, 2024