EDUCAUSE

October 15, 2024

Defense Acquisition Regulations System
Defense Pricing, Contracting, and Acquisition Policy
Office of the Assistant Secretary of Defense for Acquisition
U.S. Department of Defense

RE: Comments in response to DFARS Case 2019-D041, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements" (Docket Number DARS-2020-003 / Regulatory Identifier Number (RIN) 0750-AK81), submitted electronically at https://www.regulations.gov/commenton/DARS-2020-0034-0194

To Whom It May Concern:

On behalf of the over 2,200 colleges, universities, and related organizations that comprise the EDUCAUSE community, I would like to thank the Defense Acquisition Regulations System Office for the opportunity to comment on the proposed changes to the Defense Federal Acquisition Regulation Supplement (DFARS) covered by DFARS Case 2019-D041, which are intended to implement key provisions of the Cybersecurity Maturity Model Certification (CMMC) Program Rule addressed under Docket Number DoD-2023-OS-0063 / Regulatory Identifier Number (RIN) 0790-AL49 (https://www.regulations.gov/document/DoD-2023-OS-0063-0001).

As the nonprofit association whose mission is to lead the way in advancing the strategic use of technology and data to further the promise of higher education, EDUCAUSE encompasses higher education cybersecurity leaders and professionals with a significant interest in the application of CMMC contract requirements to higher education research projects conducted on behalf of the Department of Defense (DoD). Input from those member representatives regarding the notice of proposed rulemaking (NPRM) at hand falls into three areas:

- Fundamental research edge cases
- Unnecessary reporting overhead
- Requests for clarification

Fundamental Research Edge Cases

The brief discussion of prior comments concerning fundamental research in relation to CMMC reiterates the analysis provided by the DoD in the recent CMMC Program NPRM, specifically that fundamental research by definition does not encompass Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) and thus generally would not fall under CMMC

requirements.[1] However, the summary response of the DoD in this NPRM uses language to describe edge cases[2] in the DoD fundamental research space in a way that the EDUCAUSE research cybersecurity community finds problematic: "..., if fundamental research has the potential to become CUI, it would be subject to the requirements of CMMC."[3]

Higher education research cybersecurity leaders and professionals do not think the concept of edge cases in this area is accurately described by fundamental research possibly having "the potential to become CUI." In fact, it is not clear to our members what it means to say that fundamental research "has the potential to become CUI." Rather, if FCI or CUI became incorporated into what is ostensibly a fundamental research project, then it makes sense that CMMC requirements relevant to the data in question would apply to the handling and storage of that data. Such an occurrence would not necessarily make the research in question "CUI" or "FCI" or any less fundamental in nature; it would simply introduce the need to secure the data involved in accordance with CMMC requirements.

This discussion highlights again, however, a key point that EDUCAUSE and other higher education associations raised in our joint comments regarding the proposed CMMC Program regulations:

> …, it is incumbent upon the DoD to clearly identify the cases in which it envisions that "the information handled by contractors pursuant to the fundamental research contract activities is or will become FCI or CUI" such that "the information would be required to be processed, stored, or transmitted on an information system compliant with the appropriate CMMC Level." **Furthermore, the department should explicitly define the process it will use to reach such determinations and delineate how these unique circumstances will be communicated to DoD contract officers and specified in project solicitations.** [emphasis added] The goal of this effort would be to avoid the application of CMMC requirements in ways that conflict with the definition of fundamental research as presented in NSDD-189 and incorporated into DFARS 252.204-7000.
>
> We think that having a publicly available, comprehensive framework that catalogs and explains the bases for identifying edge cases in relation to the department's established policy on fundamental research is vital. Such a resource would ensure that all stakeholders have a common frame of reference for assessing and resolving those unusual situations. Without the proposed framework, which the DoD must work with the higher education research community to develop, researchers, institutions, and DoD contract officers will face persistent confusion about when, where, and how "information… pursuant to fundamental research contract activities is or

[1] Department of Defense, Defense Acquisition Regulation System, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)," *Federal Register*, Vol. 89, No. 158, August 15, 2024, p. 66331 (https://www.federalregister.gov/d/2024-18110/p-79).

[2] By "edge cases," EDUCAUSE means situations in which FCI or CUI finds its way into what is ostensibly a fundamental research project, such as when the DoD provides a dataset containing CUI or FCI to a project.

[3] "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation," p. 66331.

> will become FCI or CUI" in the face of established policy on fundamental research.[4]

In essence, the problematic reference in the current NPRM that is highlighted above is understandable, because, as noted in our program rule comments, effectively understanding and navigating edge cases in this space requires considerable context.

Fundamental research operates under assumptions of openness and the free exchange of ideas that do not generally apply in the more restrictive environments in which FCI and CUI are typically found. Trying to retrofit CMMC requirements into a fundamental research context once a project has been awarded has significant, negative implications for the ability of the researcher to conduct a given project and the capacity of the institution to support it from both a cost and technical/ operational standpoint. And, of course, that assumes both the researcher and institution can make the necessary adjustments at all. The impact of trying to apply CMMC requirements to a fundamental research project after it has been awarded may be so severe—it may drive the project costs so high and/or make the research itself so difficult to conduct as "fundamental research"—that the researcher and/or institution may have no choice but to decline the award. This would force the DoD to restart the entire process based on a redefined project description and with no guarantee that another suitable researcher can conduct the project at the level of funding the DoD has available. Moreover, the possibility that researchers and institutions could find themselves facing CMMC requirements in the fundamental research space could reduce the availability of researchers and institutions willing to take that chance and compete for DoD fundamental research awards.

Therefore, EDUCAUSE calls again for the DoD to engage with the higher education research and cybersecurity communities to develop a shared, publicly available framework "that catalogs and explains the bases for identifying edge cases in relation to the department's established policy on fundamental research" and supports the introduction of CMMC Program requirements only when clearly and objectively applicable. We recognize that the DoD declined to accept our recommendation regarding the development of such a framework in the recently published final rule for the CMMC Program,[5] but we hope that our additional comments on the issue in this rulemaking will encourage the department to reconsider. At a minimum, however, even if the DoD continues to decline our request for a more substantive, deliberative process in relation to this concern, it should provide its higher education stakeholders with a series of examples or scenarios in which it can see the potential for a fundamental research project to face CMMC requirements. This additional information would help institutions identify potential problems during the proposal process and factor them into their decisions concerning which projects they can reasonably pursue. It would also better enable the DoD to determine if and when it might adjust its project requests to

[4] American Council on Education, Association of American Universities, et al., "Comments in response to Docket Number DoD–2023–OS–0063 / Regulatory Identifier Number (RIN) 0790–AL49, 'Cybersecurity Maturity Model Certification (CMMC) Program,'" February 26, 2024, pp. 3-4 (https://www.regulations.gov/comment/DOD-2023-OS-0063-0301).

[5] Department of Defense, Office of the CIO, "Cybersecurity Maturity Model Certification (CMMC Program)" (Final Rule), *Federal Register*, Vol. 89, No. 199, October 15, 2024, p. 83114 (https://www.federalregister.gov/d/2024-22905/p-331).

avoid potential problems in this area that could limit the success of the contracting process and ultimately of the affected projects themselves.

Reporting Inefficiencies and Opportunities for Streamlining

On a number of occasions, the NPRM identifies requirements for contractors to report information to their contracting officer that should already be available to such officers through the Supplier Performance Risk System (SPRS). For example, the proposed revisions to DFARS 252.204-7021 would require a contractor "to complete and maintain on an annual basis, or when security changes occur, the affirmation of continuous compliance with the security requirements identified at 32 CFR part 170,"[6] while the NPRM makes clear that, "SPRS is the repository for CMMC certificates and self-assessment information at present."[7] Such an affirmation must cover the "CMMC self-assessment [or] CMMC certification for each DoD UID [Unique Identifier] applicable to the contractor information systems that process, store, or transmit FCI or CUI during contract performance."[8] Yet, when a contractor updates its affirmation as a result of a security change, the proposed regulations would mandate that it separately "notify the contracting officer of any changes in the contractor information systems that process, store, or transmit FCI or CUI during contract performance and to provide the corresponding DoD UIDs for those contractor information systems to the contracting officer."[9] Similarly, under the proposed requirements, contractors would have to report to their contracting officer the DoD UIDs for their CMMC-relevant systems even though those DoD UIDs are generated by the DoD's own SPRS and presumably available to contracting officers directly.[10]

The proposed DFARS changes would also mandate that a contractor "ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments."[11] However, given CMMC certification and self-assessment reporting requirements, as well as the previously mentioned reporting requirement regarding affirmation of continuous compliance, a subcontractor's CMMC-relevant information would likely be available in SPRS in most cases, especially as compliance across Defense Industrial Base (DIB) entities increases in alignment with the phase-in of the CMMC Program. While the NPRM notes that "[c]ontractors will only be able to access their own CMMC certificate and self-assessment information,"[12] augmenting the SPRS with functionality that would allow primary contractors to access a baseline level of information on the CMMC status of potential subcontractors would reduce the reporting overhead on all of the stakeholders in a given contract. In turn, this would allow for increased resource efficiency in pursuit of the contract's objectives.

---

[6] "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation," p. 66329 (https://www.federalregister.gov/d/2024-18110/p-26).

[7] Ibid, p. 66332 (https://www.federalregister.gov/d/2024-18110/p-95).

[8] Ibid, p. 66329 (https://www.federalregister.gov/d/2024-18110/p-26).

[9] Ibid (https://www.federalregister.gov/d/2024-18110/p-27).

[10] Ibid, p. 66328 (https://www.federalregister.gov/d/2024-18110/p-25).

[11] Ibid, p. 66329 (https://www.federalregister.gov/d/2024-18110/p-28).

[12] Ibid, p. 66332 (https://www.federalregister.gov/d/2024-18110/p-95).

Likewise, it would be a worthwhile investment of DoD resources to upgrade or augment the functionality of SPRS to allow for automatic updates of CMMC information relevant to a given contract to be provided to the contracting officer for that contract. The phase-in period for CMMC requirements limits the scope of excess reporting requirements across the DIB in the near term, but eventually the burden of manual reporting of information to the DoD (or prime contractors, as the case may be) of information that the DoD likely already has in its possession will act as a drag on resource efficiency for all concerned.

EDUCAUSE urges the DoD to use the CMMC phase-in period to implement improvements in SPRS reporting functionality, including any changes to balance ease of information distribution with contractor/subcontractor rights. This would reduce unnecessary reporting overhead related to managing CMMC requirements for DIB entities and the DoD to the extent possible.

Requests for Clarification

1. The following text appears on page 66328 of the NPRM:

> This proposed rule includes a new DFARS provision, 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements, to provide notice to offerors of the CMMC level required by the solicitation and of the CMMC certificate or self-assessment results that are required to have been posted in SPRS by the apparently successful offeror prior to award, unless electronically posted.[13]

   The closing clause of the paragraph, "..., unless electronically posted," does not have a clear point of reference, either in the identified narrative or in the regulatory provision itself. EDUCAUSE requests that the DoD clarify the meaning of this text in relation to the proposed new provision, 252.204-7YYY, so that stakeholders can easily understand how it will apply.

2. Also on page 66328, a paragraph states, "Apparently successful offerors are also required to provide, at the contracting officer's request, the DoD UIDs issued by SPRS for the contractor information systems that will process, store, or transmit FCI or CUI during contract performance."[14] However, further down the page, the text implies that the reporting of DoD UIDs must occur regardless of whether the contracting officer requests such reporting: "Require the contractor to submit to the contracting officer the DoD UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract."[15]

   The relevant regulatory provision indicates that the latter point more accurately reflects the DoD's intent: "(2) Contracting officers shall require the apparently successful offeror to provide the DoD UID(s) applicable to each of the contractor information systems that will process, store,

[13] Ibid, p. 66328 (https://www.federalregister.gov/d/2024-18110/p-19).

[14] Ibid (https://www.federalregister.gov/d/2024-18110/p-20).

[15] Ibid (https://www.federalregister.gov/d/2024-18110/p-25).

or transmit FCI or CUI and that will be used in performance of the contract."[16] Therefore, EDUCAUSE requests that the DoD ensure that the mandatory nature of DoD UID reporting, regardless of a specific request from a contracting officer, be clearly and consistently stated throughout the final rule and any associated narrative.

3. On page 66329, the text refers to a definition of "senior company official" as provided in the proposed 32 CFR 170.4 of the CMMC Program NPRM.[17] However, since the proposed 32 CFR 170.4 does not contain a definition of "senior company official," EDUCAUSE assumes that the DoD intended to refer to the definition of "affirming official" provided in the proposed 32 CFR 170.22 ("...the OSA [Organization Seeking Assessment] senior official who is responsible for ensuring OSA compliance with CMMC Program requirements").[18]

   EDUCAUSE requests that the DoD ensure that the final rule and any associated narrative accurately and consistently refer to the relevant definition of the official responsible for providing an organization's affirmation of continuous compliance.

   Assuming that the definition of "affirming official" at 32 CFR 170.22 is the correct one, the DoD may also wish to consider whether that definition provides sufficient guidance on the level of seniority the relevant official should have to serve as an "affirming official." As it assesses this concern, the DoD may find the definition of "senior accountable official for risk management" from the Computer Security Resource Center of the National Institute of Standards and Technology (NIST) to be a helpful model: "The senior official, designated by the head of each agency, who has vision into all areas of the organization and is responsible for alignment of information security management processes with strategic, operational, and budgetary planning processes."[19]

4. The discussion of the proposed revisions to DFARS 217.207, "Exercise of Options," on page 66329 indicates that the new version of the clause will direct contracting officers not to exercise options on contracts unless the contractor has a current CMMC certificate or self-assessment at the appropriate level for the contract on file in SPRS.[20] The paragraph notes that these revisions stem from the policies and procedures for incorporating CMMC requirements into DoD contracts as delineated in DFARS 204.7503(c).

   As stated in the comments on the CMMC Program NPRM that EDUCAUSE filed in collaboration with other higher education associations, however, higher education research and cybersecurity

[16] Ibid, p. 66337 (https://www.federalregister.gov/d/2024-18110/p-192).

[17] Ibid, p. 66329 (https://www.federalregister.gov/d/2024-18110/p-26).

[18] Department of Defense, Office of the CIO, "Cybersecurity Maturity Model Certification (CMMC) Program," *Federal Register*, Vol. 88, No. 246, December 26, 2023, p. 89136 (https://www.federalregister.gov/d/2023-27280/p-1410).

[19] National Institute of Standards and Technology, Computer Security Resource Center, "Senior Accountable Official for Risk Management" (definition), *Glossary of Key Information Security Terms* (Online), as of September 20, 2024 (https://csrc.nist.gov/glossary/term/senior_accountable_official_for_risk_management).

[20] "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation," p. 66329 (https://www.federalregister.gov/d/2024-18110/p-36).

stakeholders have significant concerns about whether sufficient Certified Third-Party Assessment Organization (C3PAO) capacity will be available prior to each stage of the phase-in of CMMC certification requirements to ensure that all entities will be able to fairly compete for affected contracts.[21] EDUCAUSE requests that the DoD give further consideration to the following suggestions from our CMMC Program rule comments that would help to mitigate this problem:

> …, our associations recommend that the DoD extend the timeframe for phasing in Level 2 certification requirements by an additional two years. This step would ensure that the DoD has access to otherwise competitive contractors who might face undue delays in securing certification due to a lack of available assessment professionals and/or their dependence on ESPs [External Service Providers] that need certification themselves. Another option to address this problem, which again we believe the DoD analysis significantly underestimates, would be to allow all organizations that must meet Level 2 requirements to do so via self-assessments through Phase 4 of the DoD's planned implementation of the program.[22]

5. Also on page 66329, the text notes, "...the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment methodology will be addressed under a separate DFARS Case 2022-D017, NIST SP 800-171 DoD Assessment Requirements."[23] EDUCAUSE requests that the DoD provide more public communication about when the new methodology will be available, given its importance to informing institutional practice and compliance. In particular, the DoD should indicate at the earliest possible time whether the methodology will align with NIST SP 800-171, Revision 3, since that would help institutions calibrate their research cybersecurity planning and development appropriately.

6. In response to a previous public comment concerning foreign suppliers, the DoD notes that foreign suppliers will not be exempt from CMMC requirements where they apply.[24] With this in mind, EDUCAUSE requests that the DoD clarify whether it might deem relevant international cybersecurity standards or frameworks as equivalent to CMMC and, if so, what timeline and process would govern such determinations.

7. Regarding the CMMC cost allowability discussion on page 66331, EDUCAUSE requests that the DoD reconsider whether directing stakeholders to FAR 31.201-2, "Determining allowability,"[25] is sufficient to reasonably address the confusion that contractors may have about what CMMC costs they can recover via their contracts.

---

[21] American Council on Education, et al., "Comments in response to Docket Number DoD–2023–OS–0063 / Regulatory Identifier Number (RIN) 0790–AL49," February 26, 2024, pp. 9-10.

[22] Ibid.

[23] "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation," p. 66329 (https://www.federalregister.gov/d/2024-18110/p-37).

[24] Ibid, p. 66330 (https://www.federalregister.gov/d/2024-18110/p-45).

[25] Ibid, p. 66331 (https://www.federalregister.gov/d/2024-18110/p-66).

a. The FAQ for the original "CMMC 1.0" interim rule indicated that the DoD would consider CMMC certification costs as allowable, reimbursable, and non-prohibitive. However, since the release of the proposed "CMMC 2.0" rule, that prior guidance is no longer available and we are not aware of any new guidance from the DoD on the issue. This lack of current guidance reopens the question of whether such costs will be recoverable.

b. Turning to the issue of implementation costs, relevant systems and security measures may be deployed for specific research contexts or even projects in the higher education research space and thus represent costs more clearly attributable to a given contract. CMMC currently presents such a case and therefore the need for more specificity from the DoD regarding the degree to which security costs directly related to the CMMC requirements of relevant contracts are recoverable, both in relation to FAR 31.201-2 as well as FAR 31.205-32, "Precontract costs."

8. In discussing CMMC requirements in relation to telecommunications services, the NPRM states, "Data traversing common carrier systems should be separately encrypted per NIST SP 800-171 requirement 3.13.8."[26] EDUCAUSE requests that the DoD clarify whether its interpretation of 3.13.8 indicates that systems transmitting data via end-to-end encryption over external networks would be considered "common carrier systems" for the purposes of CMMC, such that they would not fall under the program's requirements. We understand from previous DoD guidance that data traversing common carrier systems does not trigger CMMC requirements so long as it is encrypted according to Federal Information Processing Standards (FIPS). Whether such guidance would apply to standard services such as Zoom or Microsoft Teams is a relevant consideration, as the need to consider enabling end-to-end encryption of such services to avoid unnecessarily triggering CMMC requirements or purchasing separate instances of the platforms would have implications for the deployment and operation of such services at the institutional level. Without further clarification, the text quoted above could lead institutions to conclude that they must have different versions of the same platforms or services for research projects that fall under CMMC versus other institutional purposes or use CMMC-compliant platforms/services across the institution as a whole. Either case has significant fiscal and resource implications for a college or university, and how institutions decide to resolve those concerns could have a substantial impact on the higher education research capacity available to the DoD.

9. The NPRM notes that contracting officers may include the revised CMMC clause in solicitations and contracts prior to the effective date of the final rule "provided that any resulting contracts are awarded on or after the effective date of the final rule."[27] EDUCAUSE member institutions continue to find that contracting officers are taking this step, however, without adequately understanding when, for example, DFARS 252.204-7021 does *not* apply (as in the case of fundamental research projects). This experience resonates with the public comments discussed in the NPRM regarding training contracting officers, where the DoD response to stakeholder

[26] Ibid (https://www.federalregister.gov/d/2024-18110/p-71).

[27] Ibid (https://www.federalregister.gov/d/2024-18110/p-89).

requests for additional contracting officer training merely states that "contracting officers will follow the prescription language in determining when to include a contract clause."[28]

Given the regularity with which our member institutions are encountering inappropriate application of the 7021 clause, however, EDUCAUSE requests that the DoD reconsider the need for heightened contracting officer training in relation to CMMC requirements, which would ultimately save significant overhead costs for the DoD and our institutions alike. Please see also the discussion on DoD staff training concerning CUI marking as well.[29] The consistency with which our member institutions are having to work with DoD contracting officers and program staff to negotiate the removal of CUI markings from non-CUI data indicates that increased training on CUI marking could provide substantial overhead savings for both the DoD and its contractors. Likewise, our member institutions frequently encounter the transmission of CUI by DoD staff to systems not intended to handle CUI, such as standard, general-purpose email systems, which further supports the request for greater DoD staff training on CUI and CMMC requirements.

10. The NPRM section on the potential for reciprocity between Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessments and CMMC assessments cites DFARS 204.7501(c) as indicating that "...CMMC assessments will not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary,..."[30] This raises the question of whether Federal Risk and Authorization Management Program (FedRAMP) certification might be considered in lieu of CMMC certification in relevant instances. EDUCAUSE requests that the DoD clarify whether this is a possibility and, if so, how it might apply. EDUCAUSE also requests that the DoD provide specific examples in which reciprocity between "other comparable DoD assessment[s]" and CMMC has been established.

11. The proposed revisions to DFARS 252.204-7021 include a new contractor requirement to report "any lapses in information security" to the contracting officer within 72 hours of such a lapse occurring.[31] However, the proposed 7021 clause does not define "lapse in information security," leading to the impression that it may significantly broaden contractor reporting responsibilities beyond those established in 7012. EDUCAUSE requests that the DoD clarify the proposed 7021 terminology in relation to the definition of "cyber incident" as provided in 252.204-7012. If this implication is unintended, then the final rule should ensure appropriate alignment between the clauses and clarity regarding 7012 as the guiding reference for cyber incident reporting. On the other hand, if the undefined language in the proposed 7021 clause reflects a different set of considerations, then the DoD should provide much clearer, more detailed guidance on what it intends with the current text, how it relates to the seemingly similar issues addressed by 7012, and what compliance with the revised 7021 should look like.

[28] Ibid, p. 66332 (https://www.federalregister.gov/d/2024-18110/p-97).

[29] Ibid, p. 66331 (https://www.federalregister.gov/d/2024-18110/p-74).

[30] Ibid, p. 66332 (https://www.federalregister.gov/d/2024-18110/p-103).

[31] Ibid, p. 66338 (https://www.federalregister.gov/d/2024-18110/p-224).

Conclusion

EDUCAUSE appreciates the extensive effort by the DoD as reflected in the NPRM to ensure that the proposed DFARS changes reflect stakeholder input from prior public comments. In that vein, we ask that the DoD continue the progress it has made in responding to concerns about the treatment of fundamental research in relation to CMMC. In the current context, this would entail working with the higher education research and cybersecurity communities on a shared approach to identifying and addressing FCI or CUI edge cases in the fundamental research space. We also believe that a significant opportunity exists for the DoD to reduce or eliminate redundant reporting of CMMC-related information by upgrading or augmenting SPRS capabilities, and we hope that the department will pursue this avenue given the substantial efficiencies it would likely generate. Finally, our members have highlighted a number of areas in the NPRM where relatively modest clarifications or revisions would facilitate greater understanding and compliance.

EDUCAUSE and its members would be happy to contribute additional perspectives on the important issues raised by this rulemaking as the DoD might find beneficial. Please contact me (jcummings@educause.edu) if we can aid further in advancing this process.

Sincerely,

Jarret S. Cummings
Senior Advisor, Policy and
Government Relations
EDUCAUSE