(Date)

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

Rin: 0750-AJ81 (Docket DARS-2020-0034)

To be Submitted to osd.dfars@mail.mil and via www.regulations.gov

The Council on Governmental Relations (COGR), EDUCAUSE, the Association of American Universities (AAU), and the Association of Public and Land-grant Universities (APLU) appreciate the opportunity to submit comments on this interim rule that establishes how the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DOD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework will apply to Department of Defense (DOD) contracts. Our member universities have a long history of conducting research vital to our nation's defense and a strong commitment to information security. Our members remain concerned, however, that the interim final rule's provisions do not adequately account for their lack of applicability to fundamental research conducted at our institutions. We urge the DOD to revisit the rule's text and unequivocally clarify that fundamental research does not fall under the rule's CMMC or NIST SP 800-171 assessment provisions unless the government is providing such information to our institutions for the conduct of that research. This is appropriate since fundamental research activities usually do not include the federal contract information (FCI) that would require securing the minimum CMMC certification (Level 1), and they definitely do not include the controlled unclassified information/covered defense information (CUI/CDI) that the 171 assessment requirements are intended to address. Thus, achieving clarity on this issue will allow all of the stakeholders in fundamental research conducted under DOD contracts, including the DOD itself, to avoid undue inefficiency and expense.

CMMC Framework and Fundamental Research

On September 1, our associations sent Under Secretary Lord a letter expressing our concerns about the implications of the CMMC program for institutions of higher education, particularly with regard to fundamental research.[1] We urged DOD to exclude fundamental research from the CMMC program. We also urged establishment of a dialogue with DOD on the issues associated with the implications of CMMC for institutions of higher education.

[1] Letter to the Honorable Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment, from EDUCAUSE, COGR, AAU, and APLU, September 1, 2020 (https://library.educause.edu/-/media/files/library/2020/9/cmmclettereducausesept120.pdf).

These concerns have been heightened by the interim rule implementing the NIST SP 800-171 DOD Assessment Methodology and the CMMC Framework. The interim rule states that companies included in the Defense Industrial Base (DIB) must obtain at least a CMMC Level 1 certification. This includes our member institutions. The Level 1 certification (Basic Cyber Hygiene) covers the Basic Safeguarding Requirements set forth in FAR 52.204-21. In the interim rule, the DOD asserts that it is urgent for DIB contractors that have not fully implemented the basic FAR safeguarding requirements to "begin correcting these deficiencies immediately."[2]

However, these mandates overlook the fact that the FAR requirements apply to federal contract information. *Federal contract information (FCI)* is defined in the FAR as "information not intended for public release." The essential characteristic of fundamental research is that the results are intended for wide public release and dissemination in order to share and advance knowledge. The FAR basic safeguarding requirements thus are not applicable unless the government is providing such information as an input to perform the research, which is uncommon. Such provided information should be identified as part of the contract. The requirements to obtain a CMMC Level 1 certification should not apply to the large majority of fundamental research contracts since FCI is not involved.

Our member institutions share DOD's concern for the importance of cybersecurity and the need to protect our research from malicious cyber activity. However, we also appreciate DOD's stated interest in fostering the open research environment necessary for the advancement of knowledge through the wide sharing of research findings and results. Balancing research and security needs is essential to the advancement of knowledge that enhances national security. Many of the FAR requirements in fact have been implemented by our member institutions. They include, however, a number of requirements, such as those restricting physical access to the research environment or the posting of public information, that are antithetical to the open research environment necessary for the progress of fundamental research.

The focus of the NIST SP 800-171 security requirements that form the basis for the CMMC framework is the protection of CUI in nonfederal systems and organizations. The relevant DFARS clause that applies these requirements is DFARS 252.204-7012. That clause applies to the safeguarding of "covered defense information" (CDI) as described in the CUI Registry. But institutions that have received a fundamental research determination under DFARS clause 252.204-7000 by definition have no CDI. The NIST CUI requirements therefore are not applicable. We flagged this issue in our earlier letter. The discussion in the interim rule ignores the fact that the 7012 clause is self-cancelling in the absence of CDI.

---

[2] Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," *Federal Register*, Vol. 85, No. 189, September 29, 2020, p. 61518.

The result is a conceptual problem in the interim rule's attempt to apply the requirements to situations where they are not applicable. It is not clear how the new DFARS 204.75 or 7021 clause applies in such circumstances. The practical consequences are equally serious. Restricting the openness required for fundamental research threatens the ability of our institutions to achieve the objectives of their DOD-funded research. In addition, the roll out of the CMMC requirement will affect DOD-funded Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) awards. Universities are often the research partners that small businesses rely on to address the fundamental research questions related to the goals of these projects, especially in the Phase I awards. If CMMC Level 1 will be the minimum requirement for SBIRs and STTRs, regardless of whether they include FCI, it may significantly limit the number of universities who can partner with small businesses under these awards.

We believe it is imperative that DOD engage with our institutions and our member associations on the issue of fundamental research in relation to CMMC. Trying to apply the CMMC framework in the interim rule to a situation where it doesn't fit is not in our mutual interests. As noted in our previous letter, we need to establish a shared context, followed by the release of formal documentation that clearly defines how the DOD, our members, and other stakeholders (e.g., companies that often serve as primary contractors) can ensure that fundamental research activities do not face inappropriate CMMC requirements.

NIST SP 800-171 DOD Assessment Methodology and Fundamental Research

The interim rule applies an assessment methodology specifically for determining contractor compliance with the NIST SP 800-171 guidelines based on the DFARS 252.204-7012 clause. In introducing the methodology, the interim rule notice states that the 7012 clause "is included in all solicitations and contracts," and "requires contractors to apply the security requirements of NIST SP 800– 171 to 'covered contractor information systems,' as defined in the clause, that are not part of an IT service or system operated on behalf of the Government."[3] Again, though, this is to address the safeguarding of CUI/CDI in those systems. As we have discussed, this context does not apply to fundamental research, where a fundamental research determination under the 7000 clause establishes by definition that the activity in question does not involve CDI.

The interim rule does not speak to the self-cancelling nature of the 7012 clause in the absence of CDI as part of a contracted project. This omission creates confusion about whether the inclusion of the 7012 clause in fundamental research contracts will trigger the application of NIST SP 800-171 DOD Assessment requirements to those contracts (or subcontracts) even though the 7012 clause self-cancels in this context.

In the absence of greater clarity in the rule about its relevance, or lack thereof, to fundamental research, its provision on the need for contractors to have current NIST SP 800-171 DOD Assessments on file with the DOD (DFARS 252.204-7019) may lead researchers and their

[3] Ibid, p. 61505.

institutions, as well as some contracting officers, to assume that such an assessment is required even though no CUI/CDI, and therefore no 171 controls, are involved. Similarly, the rule's application of the assessment requirements to subcontracts (252.204-7020) will likely also generate confusion about those requirements among industry prime contractors, which often carve out fundamental research activities for university sub-recipients. It is common for research universities to experience prime contractors inappropriately flowing down contract requirements for fundamental research activities, leading to inefficiency and expense as institutions have to work with prime contractors to resolve those errors.

The points we raise in relation to the rule's discussion of CMMC thus apply even more so here. Fundamental research does not include CDI, so the inclusion of the 7012 clause in contracts or subcontracts for fundamental research is simply pro forma and—ultimately—has no effect. However, the mere appearance of the clause in contracts and subcontracts for fundamental research already generates inefficiency and expense as previously mentioned. We urge the DOD to avoid similar issues with the NIST SP 800-171 assessment requirements by acknowledging unequivocally in the rule that those requirements do not apply to contracts and subcontracts that do not entail CDI. Just as it would make no sense to require institutions to bear the resource drain associated with implementing 171 controls when no CDI is involved, even the modest overhead that the DOD asserts would be involved with the "Basic Assessment" under its methodology would constitute an undue burden if institutions had to file self-assessments on the implementation of security controls that do not apply to the fundamental research being conducted.

Although some may see our concerns in this respect as overstated, the following text from the interim rule notice is telling:

> While there may be some entities that have contracts that contain the clause at 252.204-7012, but never process CUI and, therefore, do not have to implement NIST SP 800-171, it is not possible for DOD to estimate what fraction of unique entities fall into this category. Assuming all of these small entities have covered contractor information systems that are required to be in compliance with NIST SP 800-171, then all of these entities would be required to have, at minimum, a Basic Assessment in order to be considered for award.[4]

In the research university environment, disparate researchers and projects with disparate needs may easily exist under the same institutional "roof." Per previous DOD guidance, the needs of research activities involving CDI may be handled through 800-171 compliant enclaves while fundamental research projects operate under security requirements appropriate to their lack of CDI. It would not be reasonable to assume that a self-assessment requirement in relation to a 171 enclave would have implications for other contracted research activities not relevant to that context. As the text above illustrates, though, such thinking may creep into the picture in

[4] Ibid, p. 61510.

unexpected and inappropriate ways if clarity on the inapplicability of the assessment requirements to fundamental research is not established upfront.

Conclusion

The higher education research community understands and respects the tremendous task before the DOD and the DIB in terms of ensuring appropriate information security to protect national security. We are committed to doing our part, and in fact many research institutions have provided national and international leadership on information security for decades. We ask, however, that the DOD not subject fundamental research at our institutions to requirements that are intended to secure information that fundamental research does not entail and that run counter to the free exchange of knowledge that forms the very basis of fundamental research.

The area of concern that we are highlighting is obviously unique within the overall DOD contracting space. Fundamental research assumes from its inception that its product will be released publicly at the earliest possible point. This creates research environments that necessarily operate with a level of openness that is largely distinct from what one would expect to find across the DIB. With that in mind, we renew our request for direct engagement between relevant DOD officials and our members so that the factors we have discussed, and the significant difficulties that will arise from overlooking them, can be appropriately shared and addressed. In the interim, the DOD should revise the interim rule to clarify that the lack of information relevant to the NIST SP 800-171 assessment methodology or the CMMC framework in the fundamental research context excuses such projects and their associated contracts from the rule's provisions.

Sincerely,

EDUCAUSE
(Contact: Jarret S. Cummings, Senior Advisor, Policy and Government Relations, jcummings@educause.edu)

Council on Governmental Relations
(Contact: Robert Hardy, Director, Research Security and Intellectual Property Management, rhardy@cogr.edu)

Association of American Universities
(Contact: Hanan Saab, Assistant Vice President, Federal Relations, hanan.saab@aau.edu)

Association of Public and Land-grant Universities
(Contact: Deborah Altenburg, Assistant Vice President, Research Advocacy and Policy, daltenburg@aplu.org

Association Descriptions:

EDUCAUSE is a nonprofit association and the foremost community of information technology leaders and professionals committed to advancing higher education. It includes over 1,800 colleges and universities, 450 corporations, and dozens of related organizations. EDUCAUSE supports IT professionals and the further advancement of IT in higher education through research, advocacy, community and network building, and professional development.

The Council on Governmental Relations is an association of 190 research universities and affiliated academic medical centers and research institutes. COGR concerns itself with the impact of federal regulations, policies, and practices on the performance of research conducted at our member institutions.

The Association of American Universities (AAU) is an association of 63 U.S. and two Canadian leading research universities that transform lives through education, research, and innovation. AAU member universities collectively help shape policy for higher education, science, and innovation; promote best practices in undergraduate and graduate education; and strengthen the contributions of leading research universities to American society.

APLU is a research, policy, and advocacy organization dedicated to strengthening and advancing the work of public universities in the U.S., Canada, and Mexico. Its 232 U.S. members include public research universities, land-grant institutions, state university systems, and affiliated organizations. APLU's agenda is built on the three pillars of increasing degree completion and academic success, advancing scientific research, and expanding engagement. Annually, member campuses enroll 4.3 million undergraduates and 1.2 million graduate students, award 1.2 million degrees, employ 1.1 million faculty and staff, and conduct $46.8 billion in university-based research.