September 1, 2020

The Honorable Ellen M. Lord
Under Secretary of Defense for
Acquisition and Sustainment
U.S. Department of Defense
3010 Defense Pentagon
Washington, DC 20301-3010

Dear Madam Secretary:

Given our shared interest in information security related to academic research, EDUCAUSE (www.educause.edu), the Council on Governmental Relations (COGR) (www.cogr.edu), the Association of American Universities (AAU) (www.aau.edu), and the Association of Public and Land-grant Universities (APLU) (www.aplu.org) have closely followed the progress of the Cybersecurity Maturity Model Certification (CMMC) program. As information about CMMC has come to light, our member universities and organizations have identified various issues that we had hoped the ongoing efforts of the Department of Defense (DOD) and the CMMC Accreditation Body (CMMC-AB) would resolve. This has not occurred so far, however, and the current and projected financial effects of the pandemic on our institutions increase the importance of initiating a dialogue with your office about our questions and concerns.

The cost increases and revenue losses that universities face due to disruptions stemming from COVID-19 continue to grow, and it remains unclear when they will stabilize. As a result, institutional capacity to absorb potentially substantial, new requirements as a result of CMMC is likely to be constrained even after the pandemic ends. It is vital, therefore, that the DOD work with research universities to ensure that the steps we take together to advance information security are appropriately scoped to the research involved. We have identified a number of points for discussion, especially in relation to how the potential new CMMC requirements might apply to fundamental research. We think they indicate that **the DOD should exclude fundamental research from the CMMC program**, and **we urge the DOD to establish a dialogue with our member institutions** to fully explore that possibility given the questions and concerns we have identified, some of which are highlighted below.

At first glance, university-based research may not seem to pose significant issues for a program targeted primarily at the defense contractor community. One might take this view given that a significant amount of the university-based research relevant to defense contracts often falls into the fundamental research category, which does not involve the controlled unclassified information (CUI) that the CMMC program seeks to cover. Primary contractors on defense projects often engage university researchers as subcontractors, however, to investigate a range of fundamental research questions across any number of academic fields. This raises questions

and concerns about the application and management of CMMC certification levels between primary contractors and subcontractors. Public statements by a relevant DOD official indicate that the certification level applied to a primary contractor will not automatically extend to its subcontractors. Instead, the official notes that the DOD will apply different certification requirements to different levels of relevant projects, such that subcontractors may only have to meet CMMC Level 1 or 2 certification based on the nature of their work with a project and the type of information it entails.[1] While we appreciate the flexibility this indicates, without additional clarification, we believe that it leaves too much room for the inappropriate application of certification requirements that are not relevant to the fundamental research activities that a project may include.

Research institutions and their information security leaders remain concerned about how determinations regarding certification levels will be made as well as how potential misapplications of certification requirements to fundamental research activities will be resolved. In our experience, it is important for firms that generally serve as prime contractors to receive this guidance as well. Our efforts as subcontractors to work with prime contractors to have the appropriate security standards applied to our project activities often meet with resistance. Without specific guidance from the DOD to the contrary, prime contractors are very likely to simply extend the security requirements for the overall project to our subcontracts, regardless of whether they apply. We believe that confusion on this point could be resolved through your office's direct engagement with our members 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. This is a critical consideration given that fundamental research by its nature depends on the open exchange of information and views across researchers and academic disciplines. With this in mind, it is our view that the DOD should exclude fundamental research from the CMMC program altogether. We look forward to the opportunity to discuss this issue with your office.

In addition to the points we have discussed, our members have a number of other questions that we believe a substantive and collaborative dialogue would likely resolve, further enabling and sustaining the positive contributions of academic research to our nation's defense. (Please see Attachment 1 for more examples.) We look forward to having this conversation with the Office of Acquisition and Sustainment, possibly including the Office of Research and Engineering and the CMMC-AB as well. Working together, we can clarify the key operational and security considerations and establish a shared understanding of how they can be managed within the CMMC framework (or where reasonable exceptions could be made). Please let us know at your earliest convenience when such a discussion could be scheduled. In the meantime, thank you for your time and consideration of these issues.

[1] Jane Edwards, "Katie Arrington: Firms Won't Need to Meet Same Level of CMMC Requirements on Contracts," *GovCon Wire*, March 16, 2020 (https://www.govconwire.com/2020/03/katie-arrington-firms-wont-need-to-meet-same-level-of-cmmc-requirements-on-contracts/).

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)

Cc: Ty Schieber, Chairman, Board of Directors, CMMC Accreditation Body

Attachment: *Select University Research/IT Community Questions About CMMC*

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 187 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. With a membership of 246 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 5.0 million undergraduates and 1.3 million graduate students, award 1.3 million degrees, employ 1.3 million faculty and staff, and conduct $49.3 billion in university-based research.

Attachment
Select University Research/IT Community Questions About CMMC

1. For university research projects that may involve CUI, what distinction will DOD make between the continuous, general interest other countries and their research communities have in academic research and actual "advanced persistent threats" that may trigger the application of CMMC Level 4 or 5 requirements in a given context (as proposed by NIST SP 800-172)?

2. How will the DOD work with the university research community to identify where waivers of certification levels/requirements would be appropriate given the research involved and develop processes for securing those waivers that all stakeholders can easily follow?

3. Will the DOD publicly define well in advance of imposing CMMC requirements the specific criteria for determining what types of contracts, grants, and/or research will be subject to the various CMMC levels?

4. If federal awards are received that include the DFARS 252.204—7012 clause, what does that mean for institutions whose awards do not involve CUI? I.e., does the mere presence of this or similar clauses mean that the award entails a specific CMMC level?