February 26, 2024

Office of the Department of Defense
Chief Information Officer
6000 Defense Pentagon
Washington, D.C. 20301-6000

RE: Comments in response to Docket Number DoD–2023–OS–0063 / Regulatory Identifier Number (RIN) 0790–AL49, "Cybersecurity Maturity Model Certification (CMMC) Program," submitted electronically at https://www.regulations.gov/commenton/DOD-2023-OS-0063-0001

To Whom It May Concern:

On behalf of the American Council on Education (ACE), the Association of American Universities (AAU), the Association of Public and Land-grant Universities (APLU), COGR, and EDUCAUSE, we would like to thank you for the opportunity to provide input from the higher education community on Docket ID: DoD-2023-OS-0063 / RIN 0790-AL49, which provides updated regulatory requirements for the Cybersecurity Maturity Model Certification (CMMC) Program based on the program revisions announced in November 2021. Our organizations are described as follows:

- ACE is the American Council on Education, the major coordinating body for American higher education. Its more than 1,700 members reflect the extraordinary breadth and contributions of public and private colleges and universities. ACE members educate two out of every three students in accredited, degree granting U.S. institutions.
- The Association of American Universities (AAU) represents 69 of America's leading research universities. Our members are public and private research universities on the cutting edge of innovation, scholarship, and solutions that contribute to scientific progress, economic development, national security, and public health.
- The Association of Public and Land-grant Universities (APLU) is a membership organization that fosters a community of university leaders collectively working to advance the mission of public research universities. The association's U.S membership consists of more than 230 public research universities, land-grant institutions, state university systems, and affiliated organizations spanning all 50 states, the District of Columbia, and six U.S. territories. The association and its members collectively focus on increasing access, equity, completion, and workforce readiness; promoting pathbreaking scientific research; and bolstering economic and community engagement. Annually, its U.S. member campuses enroll 4.5 million undergraduates and 1.3 million graduate students, award 1.3 million degrees, employ 1.2 million faculty and staff, and conduct $48.5 billion in university-based research.

- COGR is an association of over 200 public and private United States research universities and affiliated academic medical centers and research institutes. It focuses on the impact of federal regulations, policies, and practices on the performance of research conducted at member institutions and advocates for sound, efficient, and effective regulations that safeguard research and minimize administrative and cost burdens.
- As the association for advancing higher education through information technology (IT), EDUCAUSE represents nearly 2,200 colleges, universities, and related organizations. Higher education IT leaders and professionals at all levels work together through EDUCAUSE to develop and strengthen the role of technology in helping colleges and universities to achieve their missions.

The Department of Defense (DoD) has greatly refined the CMMC Program requirements in the proposed regulations, and our communities commend the department for its efforts. Our comments highlight specific points that reflect significant progress in the ongoing development of the program while also drawing attention to areas where further clarification or potential changes may be beneficial to all CMMC stakeholders. They address:

- Our appreciation for the DoD's recognition of the proper overall relationship between the CMMC Program and fundamental research, but also the work that remains to clarify the possible application of program requirements to edge cases;
- The importance of integrating prior DoD guidance on CUI designation and marking into the program regulations to improve the ability of DoD contract officers to work effectively with researchers and institutions in ensuring that CMMC Program requirements are only applied as appropriate (which would exclude fundamental research in general from those requirements);
- The need to revise the proposed rule to eliminate the inappropriate extension of CUI security requirements to Security Protection Data (SPD), or in the absence of that, to incorporate an actual definition/scope of SPD as well as the costs and downstream effects of extending program requirements to it in the DoD's regulatory analysis and program implementation;
- A call for the DoD to return to allowing Plans of Action and Milestones (POA&Ms) to cover a much broader array of assessment requirements, as well as to extend the timeframe for fulfilling a POA&M to 360 days;
- A recommendation that the DoD extend the overall phase-in period for adding certification requirements to solicitations or allow organizations to fulfill CMMC Level 2 requirements via self-assessment through Phase 4 of the phase-in process due to expected long-term challenges with assessor and assessment professional availability;
- The disconnect that will emerge between the proposed rule and the Defense Federal Acquisition Regulation Supplement (DFARS) regarding the version of NIST SP 800-171 that

institutions must follow once the latest version of 800-171 is released, which will almost certainly occur before the proposed rule is finalized; and

- A proposal that the CMMC Program regulations require the lead assessors of CMMC assessment teams to have knowledge and experience in the industry of the organization that is being assessed.

Appropriate Treatment of Fundamental Research

In prior comments[1] on the CMMC Program, our associations noted that the proposed treatment of "fundamental research"—the definition of which the DoD rightly identifies in the current rulemaking as deriving from National Security Decision Directive 189 (NSDD-189)[2]—in relation to the program ran counter to the nature of such research and the DoD's historical recognition of it. We particularly stressed that fundamental research *as designated by the department* excluded Controlled Unclassified Information (CUI) as well as Federal Contract Information (FCI). Since the necessity of securing FCI and CUI served as the justification for the CMMC certification requirements, the higher education associations argued that fundamental research projects should be excluded from the CMMC Program.

The current rulemaking notice acknowledges the validity of the points we originally raised, which we greatly appreciate. As its analysis of the public comments previously submitted stresses, "Program requirements apply only to defense contractors and subcontractors who handle FCI and CUI on an information system associated with a contract effort or any information system that provides security protections for such systems, or information systems not logically or physically isolated from all such systems."[3] The department's analysis further states that the definition of fundamental research that applies in this context excludes FCI or CUI, and thus fundamental research falls outside the scope of the CMMC Program except when "...DoD determines the information handled by contractors pursuant to the fundamental research contract activities is or will become FCI or CUI," which "may trigger application of CMMC Level requirements."[4]

While we thank the department for recognizing that fundamental research by definition does not fall within the scope of the CMMC Program, it is incumbent upon the DoD to clearly identify

[1] Comments of COGR, EDUCAUSE, the Association of American Universities (AAU), the Association of Public and Land-grant Universities (APLU), and the American Council on Education (ACE) on RIN 0750-AK81 (DFARS Case 2019-D041), "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," November 20, 2020 (https://library.educause.edu/-/media/files/library/2020/11/commentsdfarscase2019d041.pdf).
[2] Executive Office of the President, National Security Council, *National Policy on the Transfer of Scientific, Engineering and Technical Information* (National Security Decision Directive 189), September 21, 1985 (https://irp.fas.org/offdocs/nsdd/nsdd-189.htm).
[3] Department of Defense, Office of the CIO, "Cybersecurity Maturity Model Certification (CMMC) Program," *Federal Register*, Vol. 88, No. 246, December 26, 2023, p. 89068 (https://www.federalregister.gov/d/2023-27280/p-185).
[4] Ibid.

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."[5] 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. 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 will become FCI or CUI" in the face of established policy on fundamental research. (For example, please see DFARS 252.204-7000(a)(3), which notes that relevant national security policy statements and directives presuppose that fundamental research does not involve "covered defense information," which is the relevant category of CUI in this context).[6]

Providing more detailed guidance on when and how the department might determine that information involved in a fundamental research project "is or will become FCI or CUI" would help limit the possibility that contract officers, researchers, and institutions will take an overly cautious approach to DoD fundamental research projects. A lack of clarity on the issue could lead researchers and/or institutions to assume that they should house all DoD-related project activities in CUI enclaves "out of an abundance of caution." Since fundamental research projects per DoD policy do not involve CUI, minimizing the possibility that fear, uncertainty, and doubt will lead to an over-application of CUI requirements would also prevent the additional expenses associated with unnecessary cybersecurity requirements. These include upfront costs for implementing security measures when they are not appropriate for the data in question. However, they also encompass downstream compliance costs if and when a security incident arises regarding data that is inaccurately being subjected to CMMC Program requirements. In either case, resources that the DoD intended to use to meet its fundamental research needs would ultimately be diverted unnecessarily from those purposes, which is counter to the interests of all concerned.

[5] Ibid.
[6] DFARS 252.204-7000, "Disclosure of Information" (https://www.acquisition.gov/dfars/252.204-7000-disclosure-information).

Appropriate CUI Designation/Marking

The proposed 32 CFR 170.3, "Applicability," Part (d), states the following:

> *DoD Program Managers or requiring activities are responsible for selecting the CMMC Level that will apply for a particular procurement or contract based upon the type of information, FCI or CUI, that will be processed on, stored on, or transmitted through a contractor information system. Application of the CMMC Level for subcontractors will be determined in accordance with § 170.23.*[7]

To effectively implement this provision, it is essential that existing DoD guidance on designating and marking data as CUI be followed so that, as in the case of fundamental research, information and projects to which CMMC requirements do not apply are clearly recognized by DoD and contractor representatives alike. This consideration aligns with our request above for the DoD to:

- Clarify when and how it would determine that an otherwise exempt fundamental research project might incorporate FCI or CUI, which would then necessitate the application of CMMC requirements, and
- Ensure the results of such determinations are reflected upfront in solicitations such that a researcher and their institution can identify the CMMC status of a potential project well in advance of submitting a proposal.

With this in mind, our associations further request that the CMMC Program regulations reference DoD Instruction 5200.48, "Controlled Unclassified Information,"[8] and more specifically *Memorandum for Senior Pentagon Leadership, Defense Agency and DoD Field Activity Directors, "Clarifying Guidance for Marking and Handling Controlled Technical Information in accordance with Department of Defense Instruction 5200.48, 'Controlled Unclassified Information.'"*[9] We believe that these references can be appropriately included in the proposed 32 CFR 170.2, "Incorporation by Reference," and then reflected in 32 CFR 170.23, 170.3, and other areas of the proposed rule as relevant.

By adding these references to the CMMC Program regulations and highlighting them in relation to DoD program responsibilities for ensuring that the appropriate CMMC status of a given project is clearly identified, the DoD can make significant progress in streamlining proposal submission and subsequent contract negotiations. This would especially be the case in relation

---

[7] *Federal Register*, Vol. 88, No. 246, December 26, 2023, p. 89119 (https://www.federalregister.gov/d/2023-27280/p-950).

[8] Department of Defense, "Controlled Unclassified Information (CUI)," *DoD Instruction 5200.48*, March 6, 2020 (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF).

[9] Department of Defense, Office of the Secretary, *Memorandum for Senior Pentagon Leadership, Defense Agency and DoD Field Activity Directors, "Clarifying Guidance for Marking and Handling Controlled Technical Information in accordance with Department of Defense Instruction 5200.48, 'Controlled Unclassified Information,'"* April 2021 (https://discover.dtic.mil/wp-content/uploads/2021/04/USDRE-USD-IS-memo-CTI-CUI.pdf).

to fundamental research projects, where the fundamental research attachment to the "Clarifying Guidance for Marking and Handling" memo clearly indicates that "[t]he characterization as fundamental research shall occur when the project is added to the statement of work and prior to award" and any such project should be "scoped and negotiated by the contracting activity with the contractor and research performer, and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information)."[10]

Our associations consider it vital that the DoD take all possible steps to ensure that DoD contract officers do not apply CMMC Program requirements to fundamental research projects as prior guidance and the DoD's current analysis indicate would be inappropriate. Contract negotiations regarding fundamental research projects should not be needlessly burdened by the inclusion of FCI and/or CUI cybersecurity requirements that clearly do not apply. To the extent that there are other measures in addition to the ones we have discussed that might allow the DoD as well as researchers and their institutions to avoid the unnecessary delays and distractions that come with the misapplication of such requirements to fundamental research projects, we would urge the DoD to implement them along with our specific recommendations.

Concerns About "Security Protection Data"

Our organizations find that the equivalency drawn between CUI and "Security Protection Data" (SPD) in the proposed regulations is not consistent with the definition of CUI cited in the regulation and has the potential to create significant problems for institutions and researchers when projects do entail CUI. As the proposed rule notes, "*Controlled Unclassified Information (CUI)* is defined in 32 CFR 2002.4(h)."[11] The relevant section of the definition provided at that citation is as follows:

> ***Controlled Unclassified Information*** *(CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.*[12]

The proposed rule does not specifically define SPD, but rather simply identifies "log data" and "configuration data" as examples.[13] A higher education institution, as a "non-executive branch entity," would generally consider log and configuration data (and any other data like them) to

[10] Ibid, p. 4.
[11] Ibid, p. 89121 (https://www.federalregister.gov/d/2023-27280/p-1055).
[12] 32 CFR 2002.4(h) (https://www.ecfr.gov/current/title-32/part-2002/section-2002.4#p-2002.4(h)).
[13] See *Federal Register*, Vol. 88, No. 246, December 26, 2023, pp. 89121 and 89134 (https://www.federalregister.gov/d/2023-27280/p-1066, https://www.federalregister.gov/d/2023-27280/p-1375, and https://www.federalregister.gov/d/2023-27280/p-1378).

be information that it "possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency…" Essentially, we see log, configuration, and similar data as an outgrowth of normal institutional operations, and thus not specific to a particular DoD contract. We are thus uncertain of the basis on which DoD could seek to extend CMMC requirements to SPD when the relevant definition of CUI specifically excludes information like SPD in our determination.

At a minimum, the DoD must provide a clear, comprehensive definition of SPD if it seeks to continue incorporating SPD within the CMMC Program's scope. The brief parenthetical examples of SPD included in the proposed rule are insufficient to facilitate effective compliance by covered entities. Furthermore, if DoD insists on expanding the scope of CMMC to encompass data that, by definition, does not constitute CUI in our analysis, it should ensure that the compliance cost estimates it cites encompass the implementation, maintenance, self-assessment, and/or certification costs that would reasonably arise from such an expansion. To this point, SPD has not been viewed as subject to the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) guidelines, and thus it seems likely that the cost estimates provided for the proposed CMMC Program regulations do not account for it.

Treatment of "External Service Providers"

Our concern about the proposed rule conflating SPD with CUI extends to the discussion of "External Service Providers" (ESPs), where the processing, storage, or transmission of SPD by a company with which an institution has contracted "for provision and management of comprehensive IT and/or cybersecurity services" would be sufficient to pull the company into the scope of a CMMC assessment under the proposed regulations.[14] Again, the purpose of the CMMC requirements as stated in the rulemaking notice is to facilitate the security of FCI and CUI. By our estimation, however, it would not be accurate or appropriate to treat SPD *de facto* as CUI, given that the definition of CUI cited in the regulations excludes SPD in our view.

Therefore, it likewise would not be accurate or appropriate to extend an institution's CMMC assessment requirements to third-party service providers on the basis of their handling of SPD. How the institution deploys its various resources to address the security of CUI and FCI may fall within the purview of CMMC, but the assessment or certification of the institution's CUI security should not extend beyond the bounds of that deployment to service providers that may support institutional cybersecurity writ large.

Colleges and universities have diverse, multi-purpose technology environments in which general purpose cybersecurity solutions may be necessary to address a variety of needs. To the extent that those general purpose solutions may play a role, along with other resources and measures, in meeting CUI-specific security requirements, they can be evaluated within that

[14] *Federal Register*, Vol. 88, No. 246, December 26, 2023, p. 89121 (https://www.federalregister.gov/d/2023-27280/p-1066).

context, but institutions cannot afford to have their general cybersecurity service providers limited to solely those that can fulfill CMMC requirements regardless of the data or context involved. If institutions have to consider utilizing different service providers specifically because the CMMC Program regulations inappropriately treat SPD as CUI, the overall security of the institution *and of the CUI that the DoD seeks to protect* will be negatively impacted given the difficulty that will create for developing a holistic view of the threat environment facing the institution.

Status of Encrypted CUI

Finally, it would be helpful to provide clarity in the proposed rule with respect to properly encrypted CUI. It is generally accepted that encrypted CUI limits the scope of enclaves and associated SPD. It would be very helpful to specify this in the CUI Program regulations, both for clarifying the scopes of assessor activities and also for helping Defense Industrial Base (DIB) organizations in designing efficient and effective enclaves. A clearer understanding of the status of encrypted CUI in relation to CMMC Program requirements would add to the ability of the DIB ecosystem participants to effectively protect the CUI that they receive and/or generate.

Requested Changes to Plan of Action and Milestones (POA&M) Guidance

Our member institutions have raised concerns about the POA&M guidance in the proposed rule being overly restrictive as compared to the previous interim rule, which does not specify which objectives could or could not be included in a POA&M. As currently written, the POA&M eligibility requirements[15] would eliminate approximately two-thirds of the CMMC assessment objectives from being included in a POA&M, greatly increasing the chances of a certification failure when reasonable efforts could still be made to attain full compliance in a timely manner. Normal turnover in institutional technology environments and personnel may regularly produce situations in which a disconnect in relation to NIST SP 800-171 guidelines occurs as institutions adapt to those changes. It is our understanding that the current version of the CMMC Assessment Process[16] may include the limitations on which objectives are eligible for inclusion in a POA&M that the proposed rule specifies. However, we would argue that POA&Ms exist in part to help institutions bridge normal transitions in their technology environments while remaining competitive for projects where they validly should be. The heavily circumscribed set of objectives that would qualify for inclusion in a POA&M under the proposed rule likely would preclude researchers and institutions from contributing to DoD research where they appropriately could, and it may also unnecessarily increase the potential for compliance problems. With this in mind, the DoD should not incorporate into the CMMC Program regulations the proposed restrictions on the objectives that a POA&M can encompass. Leaving this issue as a matter for further discussion and development as part of the assessment process

[15] See the proposed 32 CFR 170.21 (https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program#sectno-citation-170.21).
[16] The Cyber AB, *CMMC Assessment Process (CAP), Version 1.0*, July 2022 (https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf).

will preserve necessary flexibility by making it easier to adjust course without having to undertake subsequent rulemaking processes.

Regarding the proposed 180-day timeframe in which a POA&M must be completed, we understand the DoD's vested interest in having organizations that are operating under such plans move as expeditiously as possible to fully implement them. However, the experience of our member institutions in working through POA&Ms indicates that the proposed 180-day completion period does not match the actual time an organization acting in good-faith would generally need to complete a POA&M. Many objectives that would be eligible for a POA&M under the regulations as currently proposed require coordination and collaboration across multiple parts of a college or university to address effectively. In addition, they may have implications for faculty engagement as well, which often entails extensive outreach and dialogue with those affected. The relevant activities can easily take an extended period of time to resolve, especially if multiple, interrelated objectives are in play. With all of this in mind, a completion timeframe of 360 days would be much more realistic based on the practical experience of our institutions, and most likely that of CMMC stakeholders in general. We urge the DoD to adopt a 360-day completion timeframe for POA&Ms in the final rule.

Assessor Availability Concerns

We note that it is not clear whether the DoD analysis of the estimated number of entities that will need a CMMC Level 2 Certification Assessment extends beyond prime contractors to include subcontractors and potentially affected ESPs. The total number identified in *Table 3–Estimated Number of Entities by Type and Level*—76,598[17]—does not appear to be large enough in our estimation to account for the full population of entities that might reasonably be expected to seek certification. As a result, our member institutions have serious concerns about whether the supply of qualified assessors will be sufficient in the timeframe that the DoD has proposed for phasing Level 2 certification requirements into its project solicitations. The implications of any significant number of contractors and service providers being unable to secure the certification necessary to compete for affected contracts are fairly serious for both the DoD as well as the entities unable to achieve certification within the required timeline through no fault of their own. We believe the necessity of the DoD having access to a comprehensive array of fully enabled and competitive contract organizations, both at the prime and subcontractor level, and the necessity of those organizations having access to a comprehensive array of service providers themselves, argues in favor of the department adopting a more conservative approach to introducing Level 2 certification requirements across its solicitations.

With this in mind, 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

[17] *Federal Register*, Vol. 88, No. 246, December 26, 2023, p. 89085 (https://www.federalregister.gov/d/2023-27280/p-416).

certification due to a lack of available assessment professionals and/or their dependence on ESPs 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.

As of February 26, 2024, the CyberAB Marketplace[18] shows only 169 Certified CMMC Assessors (CCAs) and 629 CMMC Certified Professionals (CCPs) serving the United States. It is entirely possible that the strengthened requirements for CCAs and CCPs in the proposed rule could require some significant number of those CCAs and CCPs to recertify. Moreover, some CCAs and CCPs have achieved their certifications so they can provide assistance with CMMC compliance in their organizations. They may not be available to serve on assessment teams in general, and thus the number of CCAs and CCPs effectively available to conduct assessments may be even lower. Given the tens of thousands of organizations that will require Level 2 certification according to the DoD's current estimate, not to mention the large population of subcontractors and ESPs that the DoD estimate may exclude, adopting a more conservative time horizon for fully implementing Level 2 certification across DoD solicitations or expanding the period in which contractors can rely on Level 2 self-assessments to meet CMMC requirements would seem to be in order.

Standards Alignment Across CMMC and DFARS

Our associations concur with the DoD decision to rely on NIST SP 800-171, Revision 2, as the foundational set of standards for the CMMC Program. We note, however, that relevant DFARS provisions, 252.204-7012 and 252.204-7020, currently require that contractors align their CUI security posture with the version of NIST SP 800-171 in effect at the time of the contract award.[19] NIST is currently in the process of finalizing Revision 3 of NIST SP 800-171, which could occur before the proposed CMMC Program regulations are themselves finalized. To avoid imposing different DFARS and CMMC Program requirements on contractors, with all of the attendant confusion and additional costs that trying to follow two different, if related, sets of standards at the same time would generate, the DoD should work to harmonize the DFARS 252-204-7012 and 252.204-7020 provisions with the CMMC Program regulations by revising the DFARS to reflect 800-171, Rev. 2, as the relevant standard. It could then revise the relevant CMMC and DFARS provisions in tandem moving forward as CMMC transitions to subsequent versions of 800-171.

[18] See https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending.
[19] See DFARS 252.204-7012(b)(2)(i) at https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting. and DFARS 252.204-7020(b) at https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements., which incorporates 252.204-7012 by reference.

Industry Knowledge in CMMC Assessments

A consistent feature of higher education comments in relation to the CMMC Program has been to stress the uniqueness of higher education research environments from other DIB contexts. As previously noted, the DoD's analysis of fundamental research in relation to CMMC Program requirements recognizes this uniqueness, but the distinctive elements of higher education research environments carry over into projects that may entail CMMC Level 1 self-assessment or Level 2 self-assessment/certification as well. The interplay between research and teaching and learning in academia, for example, often leads to student participation in DoD projects that are conducted in spaces that are significantly different from the top-down environments of corporate laboratories.

As a result, appropriately interpreting and assessing NIST SP 800-171 standards in academic contexts requires an understanding of how they are effectively applied and implemented in diverse, often discipline-specific settings. CMMC assessment leaders and professionals that are not familiar with higher education research environments may produce negative assessment findings not due to actual information security deficits, but simply because they lack experience with how security requirements are validly fulfilled in those environments. The implications of this possibility for colleges and universities are stark, however, as stalled or blocked certification processes may be the outcome, leading to the loss of research opportunities for faculty and students as well as limited options for otherwise improving our national defense.

With this in mind, we recommend that the DoD modify the requirement in the proposed rule for Certified Third-Party Assessment Organizations (C3PAOs) that concerns the composition of assessment teams (see the proposed 32 CFR 170.9(b)(13).[20] This provision should require that the "Lead CCA" for an assessment team have industry-specific knowledge and experience in relation to the industry in which the OSC in question participates. The DoD may be well-served in this regard by working with The Cyber AB and the Cybersecurity Assessor and Instructor Certification Organization (CAICO) to craft the necessary regulatory text so it is consistent with developing accreditation and training standards, and vice versa. Grounding the necessity of having industry-specific knowledge and experience when leading CMMC assessments in the CMMC Program regulations, however, will ensure that it is reflected ultimately in CMMC processes themselves. This, in turn, will maximize the potential of the CMMC Program to facilitate cybersecurity compliance across the many unique industries engaged in the DIB.

Confining the expectation of having industry-specific knowledge to the lead assessor role will mitigate the impact of the proposed requirement on the overall demand for CMMC assessment professionals. However, it will still create a limitation that will affect the availability of lead assessors to oversee CMMC assessment processes in different industries, such as higher education. The unique factors that different industries present in relation to CUI security, however, make assessment leadership that can place CMMC requirements in the context of a

[20] *Federal Register*, Vol. 88, No. 246, December 26, 2023, pp. 89125(https://www.federalregister.gov/d/2023-27280/p-1182).

given industry essential. Otherwise, OSCs may encounter unnecessary obstacles to achieving CMMC certifications and the CMMC Program may prove sub-optimal in promoting CUI security simply due to assessment teams misunderstanding the relevant industry context. Addressing this problem will generate additional assessor availability challenges, though, which reinforces the points we make above regarding expanding the timeframe for phasing in CMMC requirements or extending the length of time in which organizations in general can meet their Level 2 obligations via self-assessment.

Conclusion

Our associations again thank the DoD for specifically resolving the concerns we raised previously regarding the potential inappropriate treatment of fundamental research in relation to the CMMC Program. Clearly establishing that fundamental research projects by definition would not fall under the program will greatly assist colleges, universities, and faculty researchers by eliminating confusion about compliance obligations and allowing them to focus on meeting project requirements. The DoD must provide a much more rigorous accounting, however, of the bases on which it could determine that information involved in a fundamental research project might conceivably clear the threshold for the application of CMMC requirements, contrary to established policy, and ensure that those parameters (and especially their limitations) are commonly understood by all parties to a project solicitation.

Our member institutions also remain concerned about the lack of clarity surrounding certain other provisions of the proposed rule regarding the application of CMMC assessment/ certification requirements. We urge the DoD to reverse course on attempting to inappropriately treat SPD as CUI, given that the regulatory definition of CUI appears to exclude information like SPD. Likewise, we request that the DoD revisit the proposal to unduly restrict the assessment objectives that contractors can address through a POA&M and increase the completion timeframe for POA&Ms from 180 days to 360 days. The DoD should also harmonize the DFARS 252.204-7012 and 252.204-7020 clauses to align with the CMMC Program's designation of NIST SP 800-171, Revision 2, as the relevant CUI cybersecurity standard.

We further recommend that the DoD work with The Cyber AB and the CAICO to clearly establish a new requirement in the CMMC Program regulations regarding the composition of assessment teams. This new provision should specify that the lead assessors of CMMC assessment teams must have a reasonable degree of knowledge and experience in the industries of the organizations that they are assessing. The program regulations should also incorporate relevant DoD guidance on CUI designation and marking to minimize the potential for CUI designations/CMMC requirements to be inappropriately applied to fundamental research solicitations (whether in the prime contractor or subcontractor context).

In addition to these main points, please see the attached list of other considerations that the DoD should evaluate as it works to finalize the proposed rule.

While DoD support for small and/or resource-challenged organizations working toward CMMC assessment/certification requirements falls outside the scope of the proposed program regulations, our member institutions are pleased to see that the department's Office of Small Business Programs is providing funding for efforts to assist such entities in meeting "CMMC 2.0" expectations.[21] The higher education community that participates in the DIB also includes a number of institutions that face challenges in competing to support DoD objectives due to their size, rural location, service to underrepresented populations, and/or resource limitations. We ask that the DoD review its "Project Spectrum" initiative to see if it might be extended to provide assistance to relevant colleges and universities as well or otherwise serve as a model for a similar initiative in relation to higher education. Such support could go a long way toward ensuring that a diverse array of higher education institutions is available to address the DoD's needs both now and in the future.

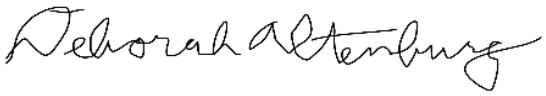
As always, our associations stand ready to work with the DoD to advance our shared interests in cybersecurity and the overall success of the CMMC Program. Please let us know if further explanation or discussion of our comments might prove useful to that effort.

Sincerely,

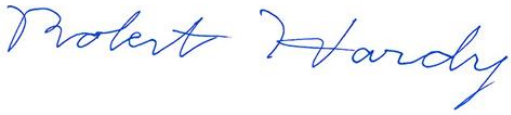
Sarah Spreitzer
Vice President and Chief of Staff
Government Relations
American Council on Education

Tobin L. Smith
Senior Vice President
Government Relations and Public Policy
Association of American Universities

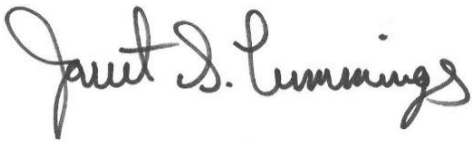
[21] Sara Friedman, "Non-profit MISI launches program to help small business prepare for CMMC 2.0," *Inside Defense*, January 19, 2022 (https://insidedefense.com/insider/non-profit-misi-launches-program-help-small-business-prepare-cmmc-20).



Deborah Altenburg
Vice President
Research Policy and Advocacy
Association of Public and Land-Grant Universities



Robert Hardy
Director
Research Security and Intellectual Property
COGR



Jarret S. Cummings
Senior Advisor
Policy and Government Relations
EDUCAUSE

Attachment

Attachment 1

Additional Considerations for Docket Number DoD–2023–OS–0063 / Regulatory Identifier Number (RIN) 0790–AL49, "Cybersecurity Maturity Model Certification (CMMC) Program"

1. The proposed regulations would benefit from a clearer explanation of the minimum certification requirement for subcontractors in relation to projects where the prime contractor must have a CMMC Level 3 certification.

    a. The proposed 32 CFR 170.23(a)(4) states that, "If a subcontractor will process, store, or transmit CUI in the performance of the subcontract and the Prime contractor has a requirement of Level 3 Certification Assessment, then CMMC Level 2 Certification Assessment is the minimum requirement for the subcontractor."

    b. The rulemaking notice does not discuss the rationale for this minimum requirement; given that the proposed rule generally indicates that CMMC certification levels will be set in relation to the FCI or CUI in question, it would help potential subcontractors if the DoD provided a clear explanation of the reasoning behind the minimum certification requirement for subcontractors in the Level 3 context.

2. Given the extensive use of the abbreviations for "Organization Seeking Assessment" (OSA) and "Organization Seeking Certification" (OSC) in the current notice, the DoD should consider explaining the distinction between OSAs and OSCs at an early point in the final rule notice to ensure greater clarity throughout the document.

3. In the proposed 32 CFR 170.2(c)(1), a reference is given as "170.98(b)" when it seems likely that it should be "170.9(b)."[22]

4. The proposed 32 CFR 170.4(b), "Definitions," includes a reference to the CISA Cloud Security Technical Reference Architecture in the definition of "Cloud Service Provider (CSP)."[23] Given the overall relevance of the CISA resource, we ask that the DoD consider whether it should be included in 32 CFR 170.2, "Incorporation by Reference," as well.

5. Also under 170.4(b), we appreciate that the DoD has provided a clear definition of "Periodically,"[24] which should help covered entities and assessment professionals alike in understanding and applying CMMC requirements.

6. The proposed definition of "Process, store, or transmit" (170.4(b)) explicitly includes residence of data in memory.[25] That factor has not been clearly identified in this context previously, and thus the DoD should highlight it consistently throughout the final rule notice

[22] *Federal Register*, Vol. 88, No. 246, December 26, 2023, p. 89119 (https://www.federalregister.gov/d/2023-27280/p-939).
[23] Ibid, p. 89121 (https://www.federalregister.gov/d/2023-27280/p-1040).
[24] Ibid, p. 89122 (https://www.federalregister.gov/d/2023-27280/p-1080).
[25] Ibid (https://www.federalregister.gov/d/2023-27280/p-1083).

and CMMC Program regulations since its overt inclusion at this juncture could raise interpretation issues in relation to existing architectures/enclaves.

7. Under the proposed 32 CFR 170.8(b)(17)(i)(E), Certified CMMC Assessors (CCAs) would be required "to disclose to Accreditation Body leadership, in writing, any actual or potential conflict of interest as soon as it is known, or reasonably should be known."[26] To ensure a clear understanding of the scope of disclosure required, both in the final rule and the accreditation body's subsequent conflict of interest policy, we recommend that the DoD provide additional detail regarding the extent to which a CCA's consulting work and/or normal duties for the CCA's regular employer would have to be reported to the accreditation body.

8. The proposed 32 CFR 170.17(a)(1), "Level 2 Certification Assessment," refers to "§ 170.14(c)(4) CMMC Level 3 Requirements."[27] Given that 170.17(a)(1) relates to Level 2 certification, however, we believe that the correct reference for the requirements that must be met is 170.14(c)(3), "CMMC Level 2 requirements."[28]

9. The "Artifact retention and integrity" sections of the proposed 32 CFR 170.17, "CMMC Level 2 Certification Assessment and Affirmation requirements,"[29] and 170.18, "CMMC Level 3 Certification Assessment and Affirmation requirements,"[30] should be made more consistent by including the reference to "unedited artifacts" in the Level 3 section in the Level 2 "Artifact retention and integrity" section as well.

10. We appreciate that the Level 2 and Level 3 assessment requirements for Cloud Service Providers (CSPs) are both set at FedRAMP Moderate. We encourage the DoD to continue looking for ways like this to maintain parallel requirements between CMMC Levels 2 and 3 so assessment and compliance processes can be streamlined to the extent possible.

11. In "Table 1 to § 170.19(c)(1)—CMMC Level 2 Asset Categories and Associated Requirements," the section on "Contractor Risk Managed Assets" includes an OSA requirement that the OSA should be prepared for such assets to be assessed against CMMC requirements.[31] However, Contractor Risk Managed Assets as referenced in the CMMC Level 2 assessment scope should be assessed in relation to the contractor's risk analysis and the controls that the contractor has determined are appropriate for such assets.[32]

---

[26] Ibid, p. 89124 (https://www.federalregister.gov/d/2023-27280/p-1148).
[27] Ibid, p. 89131 (https://www.federalregister.gov/d/2023-27280/p-1300).
[28] Ibid, p. 89128 (https://www.federalregister.gov/d/2023-27280/p-1257).
[29] Ibid, pp. 89131-89132 (https://www.federalregister.gov/d/2023-27280/p-1327).
[30] Ibid, p. 89133 (https://www.federalregister.gov/d/2023-27280/p-1361).
[31] Ibid, p. 89134 (https://www.federalregister.gov/d/2023-27280).
[32] Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, and Futures, Inc., *CMMC Assessment Scope: Level 2 (Version 2.0)*, December 2021, p. 2 (https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf).