August 24, 2022

Submitted via email to www.acq.osd.mil/cmmc and cmmcsupport@cyberab.org

Mr. Matt Travis
Chief Executive Officer
The Cyber AB
137 National Plaza, Suite 300
National Harbor, MD 20745-1153

Re: Pre-Decisional Draft, "CMMC Assessment Process (CAP)" version 1.0

Dear Mr. Travis:

This letter is to express the views of The Coalition for Government Procurement ("The Coalition") on the Pre-Decisional Draft, "CMMC Assessment Process (CAP)," version 1.0, published on or about July 26, 2022.

By way of background, The Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Its members collectively account for a significant percentage of the sales generated through General Services Administration contracts, including the Multiple Award Schedule program. Members of The Coalition also are responsible for many of the commercial item solutions purchased annually by the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for 40 years in promoting the mutual goal of common-sense acquisition.

The Coalition has over 300 members, 25% of which are small businesses. Many of our businesses have contracts with the U.S. Department of Defense ("DoD") as well as federal civilian agencies.

The Coalition fully supports the security objectives of the Defense Federal Acquisition Regulation Supplement ("DFARS") Interim Rule and the Cybersecurity Maturity Model Certification ("CMMC") program, as we recognize the importance of protecting the confidentiality of Controlled Unclassified Information ("CUI"), which is the central purpose of several DFARS clauses (252.204-7012, -7019 and -7020), as well as the CMMC 2.0 initiative. We also respect and appreciate the enormous efforts that have been made by the Cyber AB to bring the CMMC ecosystem to fruitful operation. Especially valuable has been your progress in accrediting Certified Third Party Assessment Organizations ("C3PAOs"), as they can increase the resources available to assist the Defense Contract Management Agency ("DCMA") to conduct cyber assessments under the newly initiated "Joint Surveillance" program.

We have serious reservations regarding the CAP and urge that it be withdrawn, reconsidered, and re-issued in a fundamentally different form.

1- The CAP adds more burden and expense to what is already an overcomplex process. DoD has said that approximately 70,000 companies in the Defense Industrial Base ("DIB") will be subject to CMMC Level 2, and it anticipates most of those companies will require a CMMC assessment and certification as requirements for contract eligibility. Our view, albeit unscientific, is that only a modest fraction of this very large number of companies will be able to afford the resources—personnel, technical, and financial—needed to prepare for and successfully proceed through a CMMC assessment. The CAP makes it worse.

   a. Small businesses are particularly exposed. In Senate testimony, on May 18, 2021, a DoD official explained: "Nearly all firms in the third and fourth tiers of the supply chain, or 74% of the defense industrial base, are small businesses according to the Department's contracting data." Nothing in the CAP gives any recognition, or extends any flexibility, to the assessment process when applied to small businesses. The CAP expresses a "one size is the only size" approach, and, worse, is highly prescriptive, leaving little room for discretion where skilled C3PAOs can decide what is sufficient under the specific circumstances of the organization being assessed.

   b. When DoD announced CMMC 2.0, in November 2021, its official statement described a purpose of "[s]implifying the CMMC standard and providing additional clarity on cybersecurity regulatory, policy, and contracting requirements." The CAP, however, adds complexity and obscures the process. That the draft lacks referenced templates, and introduces new terms and concepts, does not help.

   c. The U.S. Government Accountability Office recognized in a December 2021 report: "Industry—in particular, small businesses—has expressed a range of concerns about CMMC implementation, such as costs and assessment consistency." After CMMC 2.0 was announced, DoD's CMMC 2.0 website lauds its "streamlined requirements" and asserts that CMMC 2.0: "Cuts red tape for small and medium sized businesses." The CAP, by adding unnecessary and rigid assessment process requirements, contravenes this intention—and for this reason alone, DoD should step in to "rationalize" the CAP by making it simpler; more accommodating of varying contractor sizes, roles, and circumstances; closer in alignment to how DoD presently does cyber assessments; and—more importantly—less expensive and burdensome.

   d. A further complication is the likelihood that an overcomplex assessment process will make more acute the gap in availability of C3PAOs. As of this writing, there

are 21 C3PAOs, while tens of thousands of DIB companies eventually must be assessed. Contractors, when subject to CMMC 2.0 contractual requirements, can lose business if they are unable to hire a C3PAO, or must wait too long for a C3PAO to become available—irrespective of what score they may earn when assessed. This issue of assessment capacity is another reason to revise the CAP. Simplification of process requirements can reduce the time they require, enabling each C3PAO to do more assessments.

2- Issuing the CAP is premature. The first reason is that it is a wholesale departure from the regulations and standards that presently govern the cyber compliance of DIB companies who are subject to the DFARS cyber contract clauses.

a. Three DFARS presently are controlling of DIB companies who possess or use "Covered Defense Information," a term that is largely synonymous with CUI. These are: DFARS 252.204-7012, DFARS 252.204-7019, and DFARS 252.204-7020. DoD has officially disavowed any present use of DFARS 252.204-7021, the only contract clause that formally invokes "CMMC," because the CMMC 2.0 regulations are in process.

b. The -7012 clause requires a covered contractor to implement National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171, a NIST Standard intended for commercial organizations which expresses 110 "requirements," each summarized in a single sentence. NIST advises that the "requirements and controls are *tailored* to eliminate requirements . . . that are . . . [e]xpected to be routinely specified by nonfederal organizations without specification." Protecting Controlled Unclassified Information in Nonfederal Systems, at p.6.

c. In 2018 NIST published SP 800-171A to provide "federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST Special Publication 800-171," at p. ii. The -2020 DFARS clause states that the "High Assessment" to be performed by Government personnel is to use SP 800-171A.

d. Frequently Asked Questions ("FAQs") published by the DoD, for implementation of cyber requirements, reference SP 800-171A for many purposes and explain that it is to be used for both DoD Medium and High Assessments. *Id.* at A:122, p. 77. DoD has also published the "NIST 800-171 DoD Assessment Methodology (version 1.2.1) which confirms that NIST SP 800-171A is to be used for all three levels of assessment: Basic (Contractor Self-Assessment); Medium (DoD); and High (DoD On-Site or Virtual).

e. The CAP is issued by the Cyber AB and not the Government, creating concerns about primacy and authority. CMMC is cited nowhere in either the FAQs or the DoD Assessment Methodology. Whatever its value to the developing the CMMC "ecosystem," as of this writing there are *no* legally or contractually binding "CMMC" requirements, and *none* of the present, distinct CMMC documentation can be imposed on or required of DoD DIB companies (of any size or type).[1] The CAP must be clarified, simplified, and improved—and then released for discussion. Thereafter, and until the CMMC 2.0 regulations are effective, the CAP should not be required for assessment purposes; it can have other, limited uses, such as to explore or "pilot" its functionality and to learn from initial use results.

3- The second reason that the CAP is premature is that it calls for an assessment process that is legally unsupported until the CMMC 2.0 regulations are in effect—a date presently unknown and unknowable.

a. We understand that the CMMC 2.0 rules have been tendered to the Office of Management and Budget ("OMB") for consideration. The actual date that the rules are published, and their effective date, are not now known. DoD officials have spoken of their hope that "interim final rules" will be released to the public in March 2023 and become effective in July 2023. They also have acknowledged that the effective date could be a year off. The reason, we presume, is that OMB may decline to agree to another "interim final rule" and, instead, decide that a final and effective rule should follow the rulemaking "notice-and-comment" and DoD's "adjudication" of the many comments it is likely to receive once a proposed rule is published.

f. Rather than push out an incomplete CAP product, which also is premature, we urge DoD to take the time necessary to work with the AB, the C3PAO community, and other interested and informed stakeholders, to develop CAP documentation that is consistent with the CMMC 2.0 rules as and when they will be published and become effective. Today, this is impossible—since the proposed rule package, while at OMB, has not been released to the public! For now, work can proceed to improve the CAP, but there seems little point to making anyone follow the present "pre-decisional draft" document when the regulations and contract clauses may change from what DoD has submitted to OMB, and

[1] This is inclusive of the CMMC Assessment Guides and Scoping Guidance, for both Levels 1 and 2. There is much excellent content in these and related materials, but they have informational value, only, until such time as regulations are effective and companies receive RFIs, RFPs, or contracts with CMMC clauses that invoke and require their use.

when there may also be further improvements to the Level 2 Scoping Guidance and Assessment Guide.

4- In the interim, we see little value and much risk of needless expense, and confusion, by forcing assessors, and companies who are to be assessed, to follow a process and requirements that are different from what the Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC") unit of DCMA presently employs.

   a. While there is useful and informative content in 2022 CMMC documentation, including the Assessment Guides for Level 1 and Level 2 and the corresponding Scoping Guides, these are beside the point at present, since there is no legal or regulatory basis to apply or enforce any content in these Guides beyond what is expressed literally in SP 800-171 and SP 800-171A, or explained in the FAQs and DoD Assessment Methodology.

   b. Similarly, among its other problems, the CAP expresses a net new assessment process that differs greatly from what has been used by DCMA's DIBCAC unit for more than 300 DIBCAC High Assessments. It further differs from existing international standards and government accreditations such as FedRAMP. It is our position that there is no legal basis for the present "Joint Surveillance" program to employ any aspect of CMMC, including the CAP, as for now the role of the C3PAOs is to perform assessments, just as DIBCAC would do itself, under the oversight of DIBCAC.

   c. Until such time as the CMMC regulations are in effect, an assessment done "in accordance with" CMMC documentation, and using the CAP for process, stands apart from what is legally authorized. It would be misleading to companies and a potential waste of their funds, and of the efforts of a C3PAO, to do assessments against (i) future standards, which (ii) may change before the CMMC 2.0 regulations are final, using (iii) a CAP that, by its own terms, is "pre-decisional" and beset with errors and omissions.[2]

   d. While incomplete, the CAP is both different from and substantially more burdensome than the DIBCAC High Assessment Methodology, and, of course, it

[2] After the CAP is revised, and presuming approval by DoD, some companies might find it useful to engage C3PAOs to conduct "pre-CMMC" assessments. Such a "readiness" assessment would precede the effective date of the CMMC 2.0 regulations, but use the CMMC assessment and scoping documentation and be guided by the revised CAP. The revised CAP should anticipate exactly this pre-regulatory form of assessment. For example, the results would not be communicated to the Government via eMASS, and the process described at 3.1 should be adjusted so that results of such preliminary CMMC assessments are private to the organization, for its internal use only, and not disclosed to the Government.

is greatly more demanding than what DCMA does for "Medium" assessments, both of which are, unlike the CAP process, specifically authorized by DFARS 252.204-7020. We note that DIBCAC has the authority to decide which companies (and situations) merit a High Assessment, which involves either the virtual or on-site interaction of DIBCAC and the company being assessed, and where a less demanding Medium Assessment is sufficient. The necessary implication of the present regulation, and the course of conduct, is that DoD now accommodates both "Basic" and "Medium" Assessments.

e. We recommend that DoD, the AB, with the involvement of interested stakeholders, including representatives of the small business community, consider a CMMC counterpart to the "Medium" Assessment, i.e., a "CMMC-Lite," where smaller businesses, and those where less risk is presented to DoD's security objectives, will be subject to a less demanding, intensive, and expensive process.

f. The Cyber AB never should lose sight of the fundamental "business case" question that leadership of every DIB supplier will consider. This question is more acute for smaller companies and the many enterprises who provide valuable supplies and services to DoD but whose business is not dominated by DoD: Is there a return on necessary expenditure and commitment of resources? As the expense and other demands of the CMMC assessment rise, the business case is harder to close. Money wasted on unnecessary process can be better spent to achieve and sustain security.

5- Our members are concerned that compliance with CMMC is more complex, more burdensome, and more expensive than initially outlined by DoD.[3] We have observed the seemingly inexorable determination of some components of the ecosystem to add more demands and complexities to the assessment process under the guise of security. We find this trend objectionable for several reasons, and the CAP plainly will add even more aggravation and expense (but with little compensating value).

a. NIST SP 800-171 expresses every one of the 110 requirements in a single summary sentence, and accompanies each requirement with a brief Discussion, of several paragraphs. The companion document, SP 800-171A, describes the "assessment process" as "an information-gathering and evidence-producing activity." The Coalition supports the concept. For each of the security

[3] When it announced CMMC 2.0 in November 2021, DoD cited several key changes. One was "Reduced assessment costs." The Department also said: "Costs are projected to be significantly lower relative to CMMC 1.0," in part because the Department intended to "streamline requirements at all levels, eliminating CMMC-unique practices and maturity processes." The CAP, which introduces whole new processes and criteria such as the newly introduced "eligible practices for Limited Deficiency Correction."

families, -171A states the "assessment objective" and describes "potential assessment methods and objects." SP 800-171A, at 5. Importantly, the NIST publication also states:

> Organizations are not expected to employ all assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.

Id. at 5 (emphasis added). Our members are troubled that as CMMC documentation has evolved, this crucial flexibility is being replaced with excessive, binary demands that every objective be documented, and evidence of every form be created or compiled or else the organization will fail the CMMC assessment.

b. CMMC is based on SP 800-171, irrespective of whatever alternations or enhancements may be reflected in the Assessment Guides and Scoping Guidance that will have some future effect. It will be highly damaging to many, perhaps tens of thousands of companies in the DIB if CMMC is applied and enforced expecting "the most that might be done" versus what is "sufficient and can be done." The CAP underscores this concern. It is extraordinarily laborious, establishing process and procedure with density of detail that necessarily will make CMMC assessments more expensive, for assessors and assessed companies alike, and longer to accomplish. There are good reasons to question whether this, a "paint-by-the-numbers (or else) approach," will do more harm than good. DoD will be injured if CMMC's excess rigors cause smaller companies to leave the DIB or discourage innovators from selling to the that agency. Nor will it help if well-meaning companies decide to delay cyber measures because they can't afford what they fear will be required.

c. When the CAP is revised, it should be more compact, expressed more simply and clearly, and it should avoid prescription of micro steps that the C3PAOs do not need. Every C3PAO already has been vetted by DIBCAC at the High Assessment Level. Every C3PAO, presumably, has the expertise and experience to know how to set up for, negotiate the terms of, and then conduct an assessment that is "sufficient" while also "tailored" to the circumstances of the organization being

assessed. The CAP should not deny the C3PAOs of the latitude to set their own process, work with their clients, and offer assessments which are sufficient and affordable. The CAP must be reworked to drive the cost down.

6- The AB and those who've prepared the CAP are motivated to achieve "consistency," a worthwhile goal, but not the only consideration. Taken to excess—by the CAP—it produces dysfunctional consequences and costs that cannot be benefit-justified.

   a. Moreover, perfect consistency is illusory. There is enormous variation among the many thousands of companies in the DIB. It is impossible to expect that every one of these different businesses will take the same approach to all 110 NIST requirements. And NIST itself recognizes, as shown by the quote above, that they should not be expected to do so. Given the diversity of the DIB, and the variety of security problems and choices among solutions, consistency should be sought—but not demanded at any price.[4]

   b. As noted above, DCMA's High Assessment process is nothing like that described in the CAP. If it is sufficient for DoD to use with the nation's largest and most sophisticated contractors, and to accredit C3PAOs, why should the AB impose a radically more intensive and expensive process on the whole of the DIB?

   c. DoD and its contractors share an objective of having security that is "adequate" in contemporary circumstances. Indeed, DFARS 252.204-7012 (b)(3), asserts that "contractors may be required to provide adequate security in a dynamic environment." DoD should *insist* that the CMMC assessment process accommodate, and even facilitate, contractor measures that go beyond what is expected by SP 800-171 or what can be demonstrated in accordance with SP 800-171A. The CAP (and CMMC) should include flexibility to "do better" even if different. (Zero Trust, a high federal priority, is unmentioned in SP 800-171, SP 800-171A, or in the CMMC Model Overview, Assessment, or Scoping Guides.)[5]

7- The CAP is currently incongruent with existing international cybersecurity standards and we recommend the Cyber AB harmonize these issues before revising and reissuing the

[4] "Perfect is the enemy of the good," a phrase attributed to the 18th century writer Voltaire, also has been expressed as the "Pareto principle," which suggests that for many outcomes, roughly 80% of consequences come from 20% of the causes. For the CMMC ecosystem, generally, and especially for the CAP, better outcomes will result from an assessment process which focuses on the important, rather than upon all conceivable possibilities.

[5] Also to consider is that NIST in July 2022 released a "pre-draft call for comments" to lead to a Revision 3 of NIST SP 800-171. The CAP should be written to anticipate that the CMMC assessment process will change when Rev. 3 becomes effective.

document. There are sections in the pre-decisional CAP that discuss the "surrender or destruction" of "any OSC proprietary data" after the assessment. Other language requires steps to verify the "non-attribution" for interviewees during a test or demonstration. We recognize the importance of protecting sensitive and proprietary OSC data, as well as respecting the privacy of individual company personnel. Certain aspects of the CAP, however, seem consistent with ISO9001/AS9100, a Quality Management Systems standard on which a large portion of the DIB is certified. If there is a dispute after the assessment, or an audit of the assessor, evidence must be available for analysis. Further, Section 3.2.4 of the CAP outlines the destruction of artifacts after 3 years. In AS9100, all documents that are related to the product or service procured must be maintained and stored for 10 years. A CMMC Certification arguably is part of product and service conformity, as it is a contractual obligation once required by applicable contract clause requirements. Artifacts should not, in fact, be destroyed after 3 years.

8- The CAP is opaque on how companies can use Security Protection Assets; how they might expect those assets to be assessed; and what measures or evidence will demonstrate sufficient assurance regarding such assets.

a. Much of the DIB, perhaps all of it, depends upon third party products and services for their security. This will not and should not change. As matters stand, there is much left unsaid or subject to debate in the Scoping Guidance. While the CAP cannot decide upon "requirements" or establish "sufficiency," in areas where DoD has not spoken, the CAP should not impose upon C3PAOs responsibilities they are not equipped to perform, for example, determination of whether the body of evidence from a third party cloud provider is or is not FedRAMP equivalent.

b. Third party providers are relevant for all potentially CMMC in-scope assets – CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, and Specialized Assets. Following the important principle that the CMMC assessment process should "first do no harm," we strongly urge that the CAP not put C3PAOs in the position where they have to decide what requirements or process applies to such assets. This risks chaos at the operating level and contention, even dispute, between C3PAOs and their assessment clients.

c. We recommend that DoD initially take an approach to such assets that is accommodating, as considerable time and effort will be needed to answer the important and difficult questions regarding which third party assets should be subject to what requirements and how satisfaction should be determined and by whom. Taking a "draconian" position early on will preclude a huge percentage of the DIB from using Managed Service Providers, specialized security-as-a-service providers, and other third party hardware and services, that they depend upon for operations and for their current security.

In conclusion, The Coalition recommends that the AB withdraw the pre-decisional draft CAP and that the AB and DoD consider how the CAP can be changed to make it both constructive and achievable, while also deferring its use and limiting its application until the CMMC 2.0 regulations are, at minimum, publicly released. DoD and the AB also should consider establishing different levels of the CAP so that a less elaborate and expensive process is available for use with smaller companies and those who might seek a C3PAO assessment before the CMMC 2.0 regulations are effective.

The Coalition hopes you find these comments useful and thanks you for your time and consideration. Should you have any questions or concerns, please contact the undersigned at RWaldron@thegp.org or 202-331-0975.

Sincerely,