September 11, 2023

Richard Revesz, Administrator
Office of Information and Regulatory Affairs ("OIRA")
Office of Management and Budget
The White House
1600 Pennsylvania Ave. NW
Washington, DC 20500

Re: Case Number 2019-D041

VIA ELECTRONIC SUBMISSION

Dear Administrator Revesz:

The CMMC Information Institute is a 501(c)(3) educational organization dedicated to educating the American workforce, including government and government contractor personnel, about cybersecurity and related topics. We are highly supportive of the United States Department of Defense's ("DoD") efforts to enhance its supply chain security through the Cybersecurity Maturity Model ("CMMC") program. We are honored to submit these comments to the White House and hope that the comments will prove beneficial to DoD and OIRA staff as the rules associated with CMMC, including those associated with DFARS Case Number 2019-D041, (collectively the "CMMC Rules") are finalized.

NPRM vs Interim Final

As a threshold matter, we believe it is imperative that the CMMC Rules be issued as Interim Final rules. According to statistics disclosed by DoD in early 2023, less than 30% of the DoD contractors to which DoD expects DFARS 252.204-7019 and -7020 to apply had conducted a gap analysis of their cybersecurity programs against NIST SP 800-171 and submitted the corresponding scores to DoD's Supplier Performance Risk System ("SPRS"). This is true despite DFARS 252.204-7020 having been in effect for nearly a year and a half (at that time).

While this may seem like apathy on the part of many government contractors, it is actually a response to the government's current procurement approach. By awarding contracts to lowest cost technically acceptable contractors, the government incentivizes contractors who do not prioritize cybersecurity since they are able to provide their goods and services at a lower cost than those who do.

If the White House decides to publish the CMMC Rules via the NPRM process, this will send the wrong message to government contractors, and to our adversaries. Requiring the CMMC Rules to undergo the NPRM process will delay their effectiveness by many months, and possibly more than a year, as DoD adjudicates all of the responses.

While we support the public's right to comment on proposed rules, time is of the essence. Allowing the CMMC Rules to publish as NPRMs will signal to government contractors that, despite the White House's publication of several Executive Orders on the subject and the National Cybersecurity Strategy, cybersecurity simply is not a significant concern. Those same government contractors who are putting our nation at risk by waiting to implement the protections mandated by DoD's regulations will continue to reap the benefits of their inaction and will be able to underbid those who are working to safeguard the nation's Controlled Unclassified Information ("CUI").

At the same time, our adversaries are siphoning off our nation's intellectual property, personal information, and unclassified intelligence at unprecedented speeds. If DoD has to wait for the NPRM process to play out, it will only embolden our adversaries and strengthen their abilities on the battlefield. We cannot afford this at a time when those same adversaries are provoking the United States and our allies across the globe.

Due to their very nature as cybersecurity and procurement-related regulations, the CMMC Rules will inherently need refinement in the future. The time to act is now. We respectfully submit that the implementation of the CMMC program is critical to our national security and must not be delayed. The CMMC Rules should be published as Interim Final rules and allowed to take effect as soon as practical under the law. They can (and, as a practical matter, will be) always be amended later.

We also recognize that the publication of the CMMC Rules as Interim Final rules does not necessitate their immediate adoption into every DoD contract. We support DoD's plan to phase in the requirements over the next 1.5-2 years. This will give the entire ecosystem surrounding CMMC, including the CMMC Accreditation Body (the "Cyber AB"), CMMC curriculum designers, CMMC instructors, Certified CMMC Assessors, government contractors, and others, sufficient time to adapt to any changes in CMMC that may be included in the CMMC Rules while also allowing DoD to feel confident that the nation's most mission-critical CUI is being properly protected in the near term.

Allowing CMMC C3PAOs to Assess Candidate C3PAOs

One critical path toward successful implementation of the CMMC program is ensuring that there are enough Certified 3rd Party Assessment Organizations ("C3PAOs") to conduct the assessments. As of September 11, 2023, only forty-eight (48) companies have been authorized by the Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC"), in conjunction with the Cyber AB, to serve as C3PAOs. That is less than one C3PAO per state. That is simply not enough C3PAOs to meet the demand for assessments, even with a phased roll-out of CMMC.

One of the shortcomings of the current C3PAO authorization process is the limited number of assessors in DIBCAC and their need to focus on assessing other parts of the Defense Supply Chain in addition to candidate C3PAOs. DIBCAC is simply oversubscribed, and at the rate they are going it will take many years to assess the 300-400 companies who have applied to be C3PAOs. This is simply not tenable.

We respectfully submit that the current pool of authorized CMMC C3PAOs be permitted to perform assessments of candidate C3PAOs on a voluntary basis. We recognize that, some candidate C3PAOs may see it as a conflict of interest to allow another C3PAO to assess them. However, we know the leaders of several authorized C3PAOs. They have invested significantly to obtain their authorized C3PAO status. Most would not risk losing their reputation, or their investment, at such a critical time in the development of the CMMC ecosystem.

However, we also recognize that this may not be sufficient to make some candidate C3PAOs comfortable. That is why we recommend making the program voluntary. That is, current C3PAO candidates can stay in the queue for assessment by DIBCAC and avoid any perceived conflicts of interest that might arise in an authorized C3PAO assessing a potential rival. However, those candidate C3PAOs who choose to can pay a trusted, authorized C3PAO to conduct their assessment rather than wait in that queue.

This will allow the pool of authorized C3PAOs to more rapidly increase. This larger pool of authorized C3PAOs will increase competition and quickly reduce CMMC assessment costs for government contractors.

If DIBCAC or others in DoD are concerned about the quality of the assessments that will be performed by one of the authorized C3PAOs, this could be addressed by:

- DIBCAC performing random audits of the candidate C3PAOs, and/or
- DoD limiting the pool of C3PAOs who can assess other C3PAOs to those which have participated in the Joint Surveillance Voluntary Assessment program.

We would be happy to meet with White House and/or DoD staff to discuss this in more detail if appropriate.

Prioritizing Mission Critical Service Providers

Ensuring there is an adequate supply of C3PAOs is critical in part because, in addition to certifying DoD contractors who handle CUI, the C3PAOs will also be required to certify many of the Managed IT Service Providers ("MSPs") and Managed Security Service Providers ("MSSPs") who help manage and secure those contractors' IT systems. We refer to MSPs, MSSPs, consultants, and others who provide services to the nation's critical infrastructure, including DoD contractors, as "Mission Critical Service Providers." Under the CMMC program, if they are considered Security Protection Assets under the CMMC Assessment Guide, these Mission Critical Service Providers' own systems must be CMMC certified as a prerequisite for the CMMC certification of their clients' systems.

Since many Mission Critical Service Providers provide services for multiple defense contractors, we believe the CMMC Program should prioritize, and incentivize, the certification of these Mission Critical Service Providers. Such prioritization will significantly accelerate the ecosystem's ability to meet the critical CMMC requirements.

Defining FedRAMP Equivalency

Currently, under DFARS 252.204-7012, contractors who use a cloud service to store, process, or transmit DoD's Covered Defense Information (a form of CUI), must ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program ("FedRAMP") Moderate baseline and that the cloud service provider complies with certain reporting and access requirements. It is important that the CMMC Rules clearly define what is meant by "equivalency".

Many cloud service providers have strong cybersecurity programs but, because they are not government contractors, they are not eligible to obtain a FedRAMP Authorization to Operate ("ATO"). Thus, requiring a formal FedRAMP ATO will be overly restrictive and will reduce contractors' ability to leverage lower cost, but still secure, cloud services. We believe the CMMC Rules should make clear that "equivalency" can be established through:

- The creation, by the cloud service provider, of a body of evidence consistent with what would be necessary for a FedRAMP ATO and,
- a letter, issued by a FedRAMP Authorized 3rd Party Assessment Organization who has successfully conducted at least one ATO, stating that they have reviewed the cloud service provider's body of evidence and attesting that, in their professional opinion, the body of evidence would meet the requirements for an ATO.

This will allow organizations like the CMMC Information Institute to review letters of attestation and make publicly available lists of cloud services, by cloud service type, which are likely to meet the FedRAMP equivalency requirements. By acting as trusted intermediaries for services such as this, organizations like the CMMC Information Institute can serve our mission of educating clients by making it easier for them to quickly identify those cloud providers who can meet the CMMC requirements.

Clearly Differentiating Between Cloud Services and Managed Services

The CMMC Rules should also clearly distinguish between cloud services and managed services. While it is true that some service providers offer both cloud service and managed services, it is important that the CMMC Rules help contractors and the Mission Critical Service Providers to understand when the different requirements come into play. For example, if Mavis's Machine Shop (a fictitious DoD contractor) hired Perpetual Uptime (a managed service provider) to act as an MSP and MSSP on its behalf, it is presumed that Perpetual Uptime will need CMMC certification since Perpetual Uptime would be considered a Security Protection Asset under the CMMC Scoping Guide. Similarly, if Mavis's Machine Shop used Google Workspace or Microsoft 365 to author and store CUI, that service would be considered a cloud service (even if Perpetual Uptime managed the environment) under DFARS 252.204-7012.

What is unclear is whether, if Perpetual Uptime also offers offsite backup services to Mavis's Machine Shop, and that equipment is hosted in Perpetual Uptime's datacenter, whether such backup services would also be considered "cloud services" or if they are simply part of Perpetual Uptime's service. That is, it is unclear whether Perpetual Uptime would need both CMMC certification (since it is a Security Protection Asset) and FedRAMP equivalency, or whether CMMC certification alone is sufficient.

One way to address this issue is to amend DFARS 252.204-7012 to permit the cloud service to be either CMMC Level 2 certified or FedRAMP equivalent.

Clarifying Which Controls can be Inherited from a Service Provider

The CMMC Rules should make it clear when practices/requirements/objectives from a cloud service provider's CMMC certification, FedRAMP ATO, or FedRAMP equivalency attestation can be fully "inherited" from a service provider. This is a complex problem, and we would be honored to participate in crafting a proposed solution if this would be advantageous to the federal government.

Adopting the Department of Commerce's and Department of State's Encryption Exceptions for CUI

In 2016, the Department of Commerce adopted a rule which exempted from the Export Administration Regulation ("EAR") information that is "end to end" encrypted. In 2019, the United States Department of State adopted similar exceptions information that is subject to the International Trafficking in Arms Regulation ("ITAR"). Under these exceptions, if the information is end-to-end encrypted using encryption modules compliant with Federal Information Processing Standards ("FIPS") Publication 140-2 (or successors), the movement of that information outside the United States is not a deemed export. The term "end-to-end encryption" is defined as: (i) the provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and (ii) the means of decryption are not provided to any third party.

Information subject to ITAR and EAR restrictions is some of the most sensitive unclassified information handled by government contractors and the federal government. We believe that the CMMC Rules should adopt similar exceptions for at least DoD's Covered Defense Information. We also believe that 32 CFR 2002 should be amended to allow this exception for all CUI, but we recognize that 32 CFR 2002 is outside the scope of this DFARS Case.

Submission and Maintenance of Subcontractor Lists

To properly enforce CMMC, DoD will need unprecedented visibility into the Defense Supply Chain. As part of the proposal submission process, the CMMC Rules should require prime contractors to submit a list of all subcontractors to which FCI, and separately CUI, is expected to be disseminated. This will allow

DoD to ensure that all subcontractors who handle nonpublic government information have appropriate CMMC certifications and/or attestations on file. During contract performance, prime contractors should be required to maintain this list as the needs change, as contractors are added to/removed from the contract, and on at least an annual basis. The list should also distinguish between subcontractors which are authorized to access (but not remove) CUI from within a CMMC certified environment and those to which CUI is actively disseminated.

Submission of Self-Assessments and Attestations

Industry has a history of pushing responsibility for cybersecurity to low-level personnel within an organization who do not have decision-making or other executive authority in the organization (or to contractors who have similar issues). As a result, even when the personnel or contractors raise a fuss over the need for enhanced security, they are often overruled. If the CMMC Rules allow submission of self-assessment results or attestations by anyone other than a senior company official, the government will have difficulty enforcing these CMMC-related requirements because the company's noncompliance will be blamed on a junior staff member.

The CMMC Rules must be written such that only a member of the Board of Directors, the equivalent of the CEO, or a direct report of the CEO is authorized to submit any self-assessment or attestation results. The CMMC Rules should also amend DFARS 252.204-7020 to require that all submissions to SPRS be made by similarly situated individuals. This will allow for enhanced accountability throughout the Defense Supply Chain because senior management will have personal ties to those submissions.

Clarification of NIST SP 800-171 Version

32 CFR 2002 incorporates by reference the version of NIST SP 800-171 that was published in June 2015 (including updates as of January 14, 2016). 32 CFR 2002 could therefore be read as not permitting anything but that version (i.e., excluding NIST SP 800-171 Rev. 1 and NIST SP 800-171 Rev. 2) to be used as the basis for all CUI-related safeguarding requirements in contractor systems. This would include CMMC.

This creates an obvious problem, because the CMMC Rules are based on NIST SP 800-171 Rev. 2. While we recognize that 32 CFR 2002 is outside the scope of the CMMC Rules, OIRA should ensure that, as part of the CMMC rulemaking process, 32 CFR 2002 is amended to allow newer versions of NIST SP 800-171 to be used as the basis for security-related requirements in contractor systems. Failure to do so could result in expensive and distracting litigation that will significantly delay the rollout of the CMMC program.

In a similar vein, the CMMC Rules should be written in such a way that avoids a direct reference to a specific version of NIST SP 800-171. While DFARS 252.204-7012(b)(2)(i) is a laudable attempt at creating a more dynamic rule that is not tied to a specific version, it's reference to the version "in effect at the time the solicitation is issued or as authorized by the Contracting Officer" creates too much ambiguity and confusion. For example, if NIST SP 800-171 Rev. 3 is finalized on Jan. 1, 2024, that DFARS clause could be read as requiring all contractors who submit proposals for a solicitation that is issued on Jan. 2, 2024 to meet the requirements in NIST SP 800-171 Rev. 3 even if they previously obtained a CMMC certification for their environment. In addition, since the Contracting Officer has discretion to grant waivers when requested, this opens the door to contract disputes where waivers are granted for some contractors and not others. Still further, the reference to "in effect" is inappropriate since NIST Special Publications are not regulations and are not "effective"; they are merely "published" as drafts or final publications.

The CMMC Rules and/or 32 CFR 2002 should be written/amended for consistency, to remove ambiguity, and to more closely align with NIST's practices. The CMMC Rules, DFARS 252.204-7012, and 32 CFR 2002 should allow for the transition to a new revision of NIST SP 800-171 within a certain period of time (e.g., 18 months) after the final version of a new revision is published. This will allow the CMMC ecosystem (including training curricula developers, instructors, OSCs, etc.) sufficient time to adapt to the revised version.

As a practical matter, given the frequency with which NIST expects to amend NIST SP 800-171 in the future, many government contractors' systems will likely be at least one revision behind. However, from a risk management perspective, this will result in significantly better security postures than most contractors employ today.

Avoiding NIST SP 800-171 Rev. 2 and NIST SP 800-171A Rev. 1 Forced Dependencies

While the CMMC Version 2.1 documentation leak may have been unauthorized, it did highlight the fact that the Assessment Guides for CMMC Level 2 and CMMC Level 3 remain "hard-coded" to NIST SP 800-171 Revision 2 and NIST SP 800-171A Revision 1. With NIST SP 800-171 Revision 3 expected to be published in January 2024 and NIST SP 800-171A approximately six months later, it would appear DoD has either tied themselves to a legacy version of the artifacts or will have to go through some form of revisions process to the new #2 CFR Part 170 rule in order to bring them up to date.

Rather than creating verbatim copies of NIST SP 800-171 and NIST SP 800-171A, the CMMC Assessment Guides should be rewritten as supplements or appendices to NIST SP 800-171 and NIST SP 800-171A. This will allow the CMMC-related documentation to be agnostic of the revisions to NIST SP 800-171 and NIST SP 800-171 A. By not tying the CMMC Assessment Guides to specific versions of the NIST documents, DoD and can help accelerate the adoption of updated Information Security practices as they are published by NIST, such as when the threat landscape changes, or as new technologies are introduced.

Clarifying Level 1, Level 2, and Level 3 Interrelationships

CMMC Level 1 applies to the safeguarding of Federal Contract Information, whereas CMMC Levels 2 and 3 apply to the safeguarding of Controlled Unclassified Information. This means the scope of a CMMC Level 1 assessment can be drastically different from a CMMC Level 2 or Level 3 assessment.

It is unclear whether contractors must conduct a CMMC Level 1 self-assessment and submit an attestation to DoD and/or the Cyber AB before any CMMC Level 2 assessments (self-assessments or those conducted by C3PAOs) can be performed. We respectfully submit that contractors should be required to submit the CMMC Level 1 self-assessment and attestations prior to any C3PAO-conducted assessments and resulting CMMC certifications.

In addition, DoD has indicated in public comments that CMMC Level 2 certifications are prerequisites for obtaining a CMMC Level 3 assessment. DoD has also indicated that, in certain circumstances, contractors will be able to self-assess and attest that their systems meet the CMMC Level 2 requirements. The CMMC Rules should make clear whether these CMMC Level 2 "attestations" are sufficient before a CMMC Level 3 assessment can be conducted, or whether formal CMMC Level 2 certifications are required.

Self-Assessment Scores for CMMC Level 1

The CMMC Rules should create a scoring mechanism for CMMC Level 1 that is analogous to that used in the DoD Assessment Methodology for NIST SP 800-171. We respectfully submit that the CMMC Rules should change the DoD Assessment Methodology scoring system to be based at zero (0) as the lowest possible score.

The CMMC Information Institute has published an alternative scoring system, referred to as the FAR and Above scoring system, which is already in use by thousands of DoD contractors. The scoring system has been published under an open-source license and is freely available for use by DoD and other agencies. We would be happy to supply a copy of and explain the FAR and Above scoring system to the White House and/or DoD as appropriate.

While we are partial to our scoring system because it has several inherent advantages over the DoD Assessment Methodology scoring system (e.g., it allows for easy, objective comparisons of different contractors' scores, and it is easier for non-technical people to remember than a system that goes from -203 to 110), we respectfully submit that any scoring system that is created which allows Contracting Officers and prime/subcontractors to easily identify Level 1 vs Level 2 vs Level 3 scores, allows easy contrasting of contractors with similar scores (e.g., a score of 60 for a contractor at CMMC Levels 1 connotes roughly the same level of risk as a 60 for a contractor at CMMC Level 3), and is based on 0 as the lowest possible score will be much easier for contractors, service providers, Contracting Officers, Program Managers, and others to understand and apply.

Clarification of Recertification Requirements

Contractors' IT systems are constantly changing as new technologies are introduced. Even over the relatively short 3-year duration of a CMMC certification, contractors can be expected to add new hardware, software, and cloud services, and to bring onboard new Mission Critical Service Providers. The CMMC Rules need to make clear when such changes will trigger a recertification requirement for the contractors' systems. We recommend that, at least in the short term, contractors be allowed to make any changes, report them as part of annual CMMC Level 2 self-assessments and attestations. Any changes should only be subject to full recertification as part of the OSC's next CMMC certification.

Conclusion

We greatly appreciate the opportunity to provide our comments in advance of the publication of the CMMC Rules. As noted above, we sincerely believe that the CMMC program is the right path for our nation, and we offer these comments in an effort to ensure that the program can be rolled out efficiently while also addressing certain core requirements as early in the process as possible.

At the same time, we recognize the need for expedience. If addressing one of our recommendations will significantly slow the publication of the CMMC Rules, we strongly encourage DoD and OIRA to address those recommendations in future versions of the CMMC Rules.

Respectfully Submitted,

Fernando Machado (Sep 12, 2023 14:02 EDT)

James Goepel, Esq.

Co-Founder,
CMMC Information Institute
CMMC CCP, CCA, PI, PA

Fernando Machado

Contributing Member,
CMMC Information Institute