February 26, 2024

Submitted Via Email to Regulations.gov

John Sherman
Chief Information Officer
Office of the Chief Information Officer
Department of Defense
Washington, DC 20301

Re: Docket ID: DoD-2023-OS-0063; RIN 0790-AL49
Cybersecurity Maturity Model Certification (CMMC) Program
Proposed Rule 88 Fed. Reg. 89058 (Dec. 26, 2023)

Dear Mr. Sherman:

The Coalition for Government Procurement (the "Coalition") appreciates the opportunity to comment on the Proposed Rule in the above-referenced docket number and Regulatory Identifier Number (RIN) Case.[1]

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

[1] The Proposed Rule adds a new Part 170 to Title 32 CFR. We understand it to have a primary purpose of establishing the purposes of the CMMC Program and informing DoD personnel on how it should be administered. Contractual measures to implement the CMMC Program are the subject of provisions of Title 48 CFR. DoD now is working to revise the present 48 CFR treatment of CMMC, including key contract clauses. The Coalition believes it important that the DoD resources, responsible to finalize the 32 CFR Proposed Rule, and the revisions to 48 CFR, must coordinate fully to avoid creating unhelpful gaps and inconsistencies. This coordination is necessary because synchronization of these Rules is essential at the operating level, both for DoD personal and for the organizations that are subject to the Rule.

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" or "the Department") as well as Federal civilian agencies.

The Coalition fully endorses the security objectives of the CMMC Proposed Rule, 88 Fed. Reg. 89058 (the **"**Proposed Rule") and supports the CMMC framework. As discussed more fully below, however, the Coalition recommends that certain provisions of the Proposed Rule be revised and clarified. Our principal concern is that compliance with the final Rule will be prohibitively expensive such that innovative small businesses are forced out of the Defense Industrial Base ("DIB") or choose not to sell to DoD. We also are concerned that commercial item suppliers will be forced to assume expensive compliance obligations without proportionate benefits to industrial security.

A. Concerns Especially Important to Small and Commercial Businesses

1. Flexibility in Application; An Objective of Sufficiency

The DIB sector consists of over 220,000 companies, according to the Proposed Rule. Of these, DoD expects 76,598 will be subject to a Level 2 Certification Assessment, of which 56,789 (74%) are small businesses. The complex Proposed Rule, which establishes a new Part 170 in Title 32 of the Code of Federal Regulations ("CFR"), will be applied to all. It is essential that DoD build in flexibility in the application, administration, oversight, and enforcement of the Rule. This flexibility will benefit DoD and the thousands of companies subject to the Rule.

The circumstances of every business differ. The CMMC framework contemplates applying one complex rule, with even more complex surrounding documentation (Scoping and Assessment Guides, *etc.*) to all 220,000 companies, albeit at three levels. In the real world, there will be many circumstances where "perfect" compliance with one or another requirement or assessment objective cannot be achieved affordably or without unacceptable enterprise disruption.

Further, in many situations, relief from a formal requirement may be warranted where a risk assessment shows that the security gained by DoD (or by organizations subject to CMMC security requirements) is modest while the cost of 100% compliance is high. DoD specifically should explain and direct that CMMC assessors may employ their professional judgment and are not required to seek the "maximum" evidence of compliance where there is evidence of "sufficiency." Not every "assessment objective" in the

CMMC Assessment Guides, or in SP 800-171A, need be met. **Sufficiency, in the context of the business circumstances, informed by risks, is an essential proposition.**[2]

2. Clarify Access to External Services

The definitions of "External Service Providers" and "Cloud Service Providers" must be clarified to facilitate continuing access by small and medium-sized businesses ("SMBs"), especially, to external security services. Already, a very large percentage of SMBs rely upon Managed Service Providers ("MSPs") and Managed Security-as-a-Service Providers (MSSPs) for day-to-day management of their information technology ("IT") systems to handle data and system security and to respond to security incidents. The Proposed Rule can be read to apply Federal Risk and Authorization Management Program (FedRAMP) Moderate cloud security requirements to many of these external service providers. **This approach is unnecessary, unaffordable, and impracticable.**

Few of the tens of thousands of SMBs would be able to afford third party services if limited to those available today, or soon, which have received FedRAMP Moderate authorization. Enduring the FedRAMP process, with or without a Joint Authorization Board ("JAB") Provisional Authorization or Agency Authorization to Operate, is a ***very*** expensive and ***slow*** process. FedRAMP helps federal agencies to establish that the cloud services they use are compliant with the statutory requirements of the Federal Information Security Modernization Act ("FISMA"). But FedRAMP never was intended to apply to offerings of *commercial* cloud services, by *commercial* cloud providers, to

---

[2] We note that the Proposed Rule describes the Cybersecurity Maturity Model Certification Assessment Guides as "optional resources to aid in understanding" and states that they "provide supplementary information … [, but] do not identify specific solutions or baselines." 88 Fed. Reg. 809075. Yet, our member companies are concerned that too many cyber advisors, and eventual CMMC assessors, will take an approach that equates every one of the approximately 320 "Assessment Objectives," as are listed in SP 800-171A and the CMMC Level 2 Assessment Guide, to a "requirement" that is the subject of separate evidentiary documentation. This approach is too much process (and too much expense), and it aggravates the cost problem faced by thousands of small and medium sized businesses ("SMBs"). DoD should state clearly, in the Final Rule, that assessors may consider -171A, and the CMMC Assessment Guides, but are given the discretion to use their judgement, informed by contractor circumstances, to decide when sufficient measures have been taken to meet a security requirement and to satisfy the overall objective of assessment.

commercial companies who happen to supply goods or services to DoD, but who do not operate systems by or on behalf of DoD.

As DoD works to finalize the 32 CFR Proposed Rule, and to update its 48 CFR counterpart, it should avoid draconian consequences on the thousands of small businesses who depend upon CSPs, MSPs, MSSPs and other External Service Providers ("ESPs"). DoD also should recognize that the community of ESPs is largely comprised of small businesses. DoD's should strike a balance between imposed security requirements, on the one hand, and the ability of thousands of DoD suppliers to afford satisfaction of those requirements.

There should be no misunderstanding of the dysfunctional consequences of an excessively restrictive approach to ESPs generally. SMBs and other contractors must have confidence that they will pass a CMMC assessment using such resources. Without that confidence, one choice is to migrate their IT and security functions to the relatively small number of expensive providers of solutions already authorized at FedRAMP Moderate or higher. For many, this is unaffordable and presents an intolerable operational disruption. Companies will face pressure to return to internal measures, where they seek to protect information with systems, applications, and personnel who are on-premises. Even assuming such businesses have the resources (financial, technical, and human) to satisfy CMMC security requirements on their own, this will produce a worse security outcome versus today's norm, where many system and security functions are outsourced.

It is inarguable that most SMBs rely upon one or another form of cloud-based managed or security services. The clock cannot be "turned back" to on-premises security internally provisioned, as doing so runs against the grain of contemporary experience across public and commercial sectors. This is a condition with the highest likelihood of causing some SMBs to exit the DIB, where they cannot afford to comply, and innovators will decline to contract with DoD.

3. Means of Assessment of External Service Providers

The Proposed Rule, 88 Fed. Reg. at 89066, states that if an Organization Seeking Assessment ("OSA") "utilizes an ESP, other than a Cloud Service Provider, the ESP must have a CMMC certification level equal to or greater than the certification level the OSA is seeking." In essence, an OSA which seeks a CMMC Level 2 Certification Assessment must validate that an ESP it uses has a CMMC Level 2 Certification Assessment.

There is no present means to accomplish such an assessment. Today, the Department's Joint Surveillance Assessment program ("JSV"), conducted jointly by the Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC") unit of the Defense Contract Management Agency, and CMMC Third Party Assessment Organizations (C3PAOs,) is only available to defense contractors who have both the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and Controlled Unclassified Information ("CUI"). As presently proposed, the CMMC rules also will be limited to **contractors,** as CMMC certification requirements will be imposed, we expect, by a revised DFARS clause 252.204-7021. ESPs (inclusive of most CSPs, MSPs, and MSSPs) ordinarily are service providers to whom the -7012 clause, and CMMC contractual obligations do not flow down. This means, in turn, that there is no mechanism for ESPs to demonstrate that they satisfy the requisite "CMMC certification level."

Perhaps, DoD expects the Cyber AB to establish the needed mechanism. If so, the authorization and direction to do so should be made explicit in the Final Rule. Also, DoD should act to assure that ESPs, and the contractors who are their clients, are not put through repeated, serial demonstrations of sufficiency. This would be a costly and disruptive duplication of efforts. The assessment mechanism for ESPs should produce a certification or other publicly accessible, reliable documentation such that clients are not required to establish the credentials for ESPs who have been previously and successfully assessed.

As noted, language in the Proposed Rule would require an ESP to have the same certification level as that sought by the OSA. We support measures to assure the security of all forms of ESPs. We think an appropriate starting point is to use the same baseline requirements of National Institute of Standards and Technology ("NIST") SP 800-171 Rev 2 and to assess against the related CMMC security requirements. The security issues present for different classes of ESPs (MSPs, MSSPs, cloud-delivered security applications, *etc.*), however, are distinct from those of enterprises seeking to protect the security of CUI they employ in performing DoD contracts. We expect that the best, cost-optimized solutions, also differ. We strongly encourage DoD to form one or more public-private partnerships to develop control sets based on NIST publications that are tailored for different types of ESPs, and which focus upon the confidentiality objective of CUI.

4. Clarify Treatment of ESPs vs. CSPs.

The Proposed Rule, at § 170.19(c)(2), states that "if an OSA utilizes an External Service Provider (ESP), **other than a Cloud Service Provider (CSP),** the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the

OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment." (Emphasis added.)

Initially, it is important to clarify the distinction between an "ESP," whose services may be hosted on and delivered from a cloud, and a "CSP." The Proposed Rule can be read to treat all ESPs, including MSPs and MSSPs, together, and, as cited, to apply CMMC Level 2. If, however, such ESPs *are* considered by DoD or assessors to be CSPs, then greatly different requirements may apply. The potential for confusion must be resolved by additional explanation and clarification.

The Office of the Chief Information Officer (OCIO) issued a Memorandum on FedRAMP equivalency dated January 2, 2024. The underlying DFARS clause, at 242.204-7012(b)(2)(ii)(D), obligates a subject contractor, where it "intends to use an external cloud service provider to store, process, or transmit any covered defense information" in contract performance, to "require and ensure" that the CSP meets security requirements "equivalent to those" established by the Federal Government for FedRAMP Moderate.

Many, if not most, ESPs *are* cloud hosted, and this hosting includes security applications delivered by MSPs and MSSPs. In the simplest case, where these applications never "store, process, or transmit" any Controlled Defense Information (CDI), they would not become subject to the demands of FedRAMP Moderate – according to the OCIO Memorandum. It is not uncommon, however, for such services and applications to have occasional, limited, or greater contact with CDI of their clients. This contact seems especially likely where MSPs, for example, offer "enclave" solutions that host and transmit CDI. Are these situations where, invariably, all the obligations of FedRAMP Moderate must be satisfied? The Coalition hopes not.[3]

FedRAMP Moderate is the product of longstanding efforts by the Executive Branch to satisfy FISMA as to the confidentiality, integrity, and availability of federal information when federal agencies use cloud applications, platforms, or infrastructure. The situation here is profoundly different, as we address commercial organizations (ESPs, such as such as MSPs or MSSPs) who provide IT and security services to other commercial organizations (contractors subject to CMMC assessment) who have the important, but

[3] DoD should offer guidelines for CMMC-suitable enclaves and should facilitate robust competition among private sector offerors of such enclaves. We have no objection to DoD pilots of enclave solutions for SMBs, but we believe the private sector can address these needs better, faster, and with the benefit of price and feature competition.

limited, obligation to secure the confidentiality of CDI, under DoD. These contractors do *not* operate information systems "by or on behalf of" DoD. Analytically, therefore, and legally, it is neither necessary nor prudent to graft FedRAMP Moderate requirements upon such ESPs.

Yet, grafting is exactly what may occur unless the OCIO January 2 Memorandum is rescinded or revised and reconciled with the conflicting language in the Proposed Rule. The OCIO Memorandum would seem to treat as a CSP, subject to FedRAMP Moderate, any cloud-based ESP that has contact with CDI, irrespective of the nature, frequency, or amount of such contact, or other controls employed by the ESP.[4]

If cloud-based ESPs are broadly found to be CSPs and subject to the FedRAMP Moderate demands as interpreted by the OCIO Memorandum, there will be a virtual "catalogue" of adverse, and presumably unintended, events injurious to the defense industry, to service providers, and to DoD itself. As discussed above, the defense industry will be pushed to return to "on premises" IT system management and data security. Competition and innovation among ESPs will be squelched. Costs to use ESPs, where clients can find a service that meets the FedRAMP Moderate demands of the OCIO memo, will skyrocket. No more than a tiny fraction of existing ESPs will contemplate the lengthy FedRAMP process, very high costs of Preliminary Authorization (much less a separate Agency ATO, if required), the elaborate document set, and the cost of hiring 3PAOs for their review and assessment. Only in a very few cases will there be a plausible "business case" – either for ESPs, to make such at-risk investments, or for DIB companies to hire ESPs who cannot show satisfaction of the very high bar.

Wholly apart from the cost consequences to thousands of DIB contractors, as they shed ESPs, there will be great disruption in business continuity and efficiency. That disruption will impact adversely performance of DoD programs and missions. DIB security actually will be reduced since it is rare, today, that SMBs on their own can accomplish as much to establish and sustain security as ESPs enable.

---

[4] In fact, in several respects the OCIO Memorandum raises the bar above what is required by FedRAMP Moderate for CSPs who deliver Cloud Service Offerings ("CSOs") to federal customers. The OCIO Memorandum requires 100% compliance with the FedRAMP Moderate security baseline, which consists of approximately 325 controls (if NIST SP 800-53 Rev 4 is applied). The OCIO Memorandum allows no POA&Ms. Both are departures from the ordinary process of FedRAMP authorization.

DoD must clarify what ESPs are to be treated as CSPs and, in doing so, must give greater latitude for ESPs to have a cloud basis, connection, and means of service delivery. DoD must establish what security principles are *necessary* and *sufficient* for ESPs. These must not be FedRAMP Moderate, but they may differ, eventually, from the present SP 800-171 baseline which was written largely for contractor on-premises IT management. This approach may call for revision to the referenced "or equivalent" language in the - 7012 provision which is within Title 48 CFR that is also under revision. Still another possibility to consider is a further "relief period," within which, OSAs and Organizations Seeking Certification ("OSC") document the security measures of the ESPs they use so that these can be considered by assessors without requiring immediate compliance with SP 800-171 or FedRAMP Moderate.[5] If service providers are required to provide such documentation, perhaps with DoD guidance on key issues to address, such as the Customer Responsibility Matrix, it will help organizations to make informed, competitive selection decisions among candidate ESPs.

5. Expand Use of Self-Assessments for Level 2

DoD projects that 80,598 companies will be subject to Level 2 CUI protection requirements over the 7-year phase-in period. Table 6, 88 Fed. Reg. 89086. Of these, 4,000 (5%) will be permitted to self-assess, while 76,598 (95%) will require a certification assessment. First, DoD should clarify how it will determine which companies need only to self-assess. There should be **sufficient information in the Rule** so that companies have a reasonably clear basis to anticipate, when it becomes effective, whether they will require a certification assessment. Here, we urge DoD expressly to use its internal **risk assessment** methodologies to consider the nature of CUI held by companies, the sensitivity of that information, and the significance of adverse impact to the Department if the confidentiality of such information was compromised. Not all information, even where it is clearly designated as CUI, has the same security importance to DoD.

Second, DoD should increase the number of Level 2 companies for whom self-assessment is permitted. The potential shortfall in qualified assessment organizations

---

[5] Regarding SP 800-171, DoD should appreciate that the assessment documents, SP 800-171A, and the CMMC Level 2 Assessment Guide, were not tailored for the many variations of ESPs and the security issues presented by their forms and methods of service. For this reason, DoD should work actively with private sector stakeholders to develop security templates that fit representative external services models and to establish an ongoing process to promptly address security questions regarding ESPs as they arise.

and assessors (C3PAOs, CCAs and CCPs) itself may dictate such a change. Even before the effective date of the CMMC Rule, there is pressure as more companies in Level 2 seek assessment when the number of credentialed assessors is far short of demand. The number of such assessors is a pacing function for the Level 2 roll-out.

6. Reduce Level 1 Demands

DoD estimates that 103,010 companies at Level 1 will self-assess over the 7-year implementation period. 88 Fed. Reg. 89105. We believe the cost estimations in the Proposed Rule greatly understate the costs and burdens of Level 1 compliance, at least as that is expected by DoD. The Proposed Rule, at § 170.15(a)(1), requires that seventeen (17) requirements be "MET" and does not allow for POA&Ms. It also states, at § 170.15(c)(i):

> "The CMMC Level 1 Self-Assessment **must be performed using the objectives defined in NIST SP 800–171A** (incorporated by reference, see § 170.2) for the security requirement that maps to the CMMC Level 1 security requirement as specified in table 1 to paragraph (c)(1)(ii) of this section. In any case where an objective addresses CUI, FCI should be substituted for CUI in the objective.
>
> (Emphasis added.)

The Coalition believes that few companies who are or will become subject to these CMMC requirements for Level 1 have any idea of what is expected of them and that most of these companies will struggle with the necessary resources (financial, technical, and human). The 17 enumerated requirements are derived from FAR 52.204-21 (the "Basic Safeguarding" clause), which widely appears in federal contracts. It has not been successfully or broadly communicated that *DoD's* enforcement of this clause will require use of the *assessment methodology* of SP 800-171A, or that of the corresponding and applicable CMMC Assessment Guide. The *actual costs* of demonstrating satisfaction of these control objectives in accordance with the specified assessment objectives is *much* greater than presently anticipated by the companies that will be affected. Nor do these companies appreciate the *measures* they will be required to take, even if cost is not a barrier.

We believe these demands are excessive in terms of cost and burden relative to value. Level 1 does not involve "Controlled Unclassified Information." Rather, it involves "Federal Contract Information," which may be less consequential in terms of

importance or impact should confidentiality be compromised. We urge DoD to remove Level 1 entirely from the CMMC framework and program, or to defer Level 1 implementation for several years. As the FAR Basic Safeguarding clause is in many federal contracts, the underlying contractual obligations are present and potentially enforceable. There is insufficient gain, and too much "pain," to include Level 1 in the CMMC enforcement program at present.

7. COTS and Commercial Items

The Proposed Rule, 88 Fed. Reg. 89106, states that it will impact small businesses that do business with DoD "except for contracts or orders that are exclusively for COTS items or valued at or below the micro-purchase threshold."[6] Even so, the Proposed Rule raises several concerns for COTS items and more for commercial items.

- DoD should make clear, in the Final Rule, that COTS suppliers are not now subject to any CMMC requirement (including Level 1). (Doing so will dispel any concern among COTS suppliers that they will be obliged to provide affirmations or undergo compliance assessments.)

- DoD should inform prime contractors that they should not, as a matter of course, flow down CMMC requirements to COTS suppliers who may be in their supply chain.

- Contracting Officers, and other DoD oversight and administrative officials, such as persons at DIBCAC or DCMA, should be instructed not to apply CMMC requirements to COTS suppliers.

- DoD should affirm that the FAR definitions of COTS (and commercial service), at FAR 2.101, apply for purposes of the CMMC Rule.

- Regarding providers of commercial items and services, we question whether the expected costs and burdens of CMMC compliance, even if limited to Level 1 where only FCI is present, are justified by the actual

[6] This is consistent with DFARS 204.7304, which limits the application of the DFARS cyber clause, 252.204-7012, where solicitations and contracts are solely for the acquisition of COTS items.

security benefit either to the Department or to contractors. *See* our recommendation A.6, above.

- We appreciate that there may be concerns regarding the supply chain integrity of COTS or commercial suppliers. The CMMC rules, which are to protect the confidentiality of CUI, are not the vehicle to address such concerns. No presumption should be made that any COTS or commercial item supplier has CUI or FCI.

B. Other Recommendations

1. POA&Ms

DoD limits the number of control requirements on which POA&Ms are permitted and requires close-out within six (6) months. DoD should review the requirements for which POA&Ms presently are not allowed and consider whether it can allow POA&Ms for more requirements. Where POA&Ms are required, DoD should establish a mechanism to permit a longer close-out period.[7] DIBCAC and DoD itself have the explicit authority to take a more flexible approach to POA&Ms. Making the rule too demanding and too rigid risks a "disconnect" that could make compliance impossible for hundreds, if not thousands, of companies in the DIB, raising the risk that some companies exit the DIB and others (innovators) decline to enter the DIB, all of which raises considerable risk to supply chain continuity on existing programs.

2. Scope of Delegation to the Cyber AB

We appreciate that the scale of the CMMC program explains the broad delegation of responsibilities and authorities to an Accreditation Body (presently the Cyber AB). Generally, we support the work of the Cyber AB and believe it has done a good job in launching a program to train and accredit both cyber advisors and various levels of assessors. We have concerns, however, that the rate of growth of accredited assessors will be much behind the rate of growth of demand for assessment services. DoD should consider allowing C3PAOs to issue interim or conditional certifications if they are unable to timely and fully process contractor applications for certification. Contractors should not be barred from receiving awards in such situations. DoD further should consider whether it can provide

[7] DoD should consider allowing up to a year to close out noncritical areas of POA&Ms.

financial assistance to the Cyber AB to provide it financial stability and to help accelerate its process of training, testing, and accreditation.[8]

Relatedly, the Proposed Rule has delegated complete authority to the Accreditation Body to resolve differences or disputes as may arise between an OSA or OSC. Looking at Proposed Rule § 170.8, each C3PAO is required to have an internal appeals process. This requirement may not be realistic for smaller C3PAOs. Where the C3PAO is unable to resolve a dispute, it is escalated to the Accreditation Body which, according to Proposed Rule § 170.8(b)(16), is to "[r]ender a final decision on all elevated appeals."

DoD should have a role in the disputes process. Companies who fail a required certification assessment process may or will be ineligible for contract award. The compliance obligations are complex and rarely the subject of uniform interpretation by all concerned. Under these circumstances, disagreements, with real money at stake, are inevitable, as is escalation of disputes to the Accreditation Body.[9] The resolution of such disputes will determine eligibility for government contracts. DoD should assume responsibility to review AB determinations and be the final arbiter of the results. DoD also should articulate an internal process for such review and communicate that process to private stakeholders.

Should DoD insist that these functions be performed by an external third party, we see some risk of legal challenge. We recognize that DoD states, Proposed Rule at § 170.1(e), that the new Part 170 of 32 CFR "creates no right or benefit, substantive or procedural, enforceable by law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person." Where economic interests and contractual opportunities are at stake, this disclaimer may be challenged legally, and such a challenge, until resolved, would introduce uncertainty not helpful to the CMMC framework and program objectives.

3. Level 3 Concerns

The Proposed Rule provides little insight into what criteria or process will govern the determination of when a solicitation or contract will require a Level 3 certification assessment. DoD estimates that just 1,487 companies will be subject to Level 3 certification

---

[8] If the Cyber AB cannot timely meet its responsibilities, additional time should be built into the phased approach.

[9] That the Cyber AB will have additional dispute resolution responsibilities is a further reason to find ways to provide it with further financial support.

requirements. This represents less than 1% of the total number of companies subject to CMMC requirements and just 2% of the companies who will be subject to Level 2 requirements. DoD should improve its explanation of what factors and considerations it will employ in deciding when to require Level 3. At present, there is little guidance. Level 3 is intended to provide better protection against Advanced Persistent Threats ("APT"), but these APT threats potentially may be directed to a much larger group of companies than just 1,487 companies. Also, we note that there are policy considerations, for program managers, articulated at Proposed Rule § 170.5(b):

> (b) Program managers and requiring activities are responsible for identifying the CMMC Level that will apply to a procurement. Selection of the applicable CMMC Level will be based on factors including but not limited to:
>
> (1) Criticality of the associated mission capability;
>
> (2) Type of acquisition program or technology;
>
> (3) Threat of loss of the FCI or CUI to be shared or generated in relation to the effort;
>
> (4) Potential for and impacts from exploitation of information security deficiencies; and
>
> (5) Other relevant policies and factors, including Milestone Decision Authority guidance

These may be helpful for DoD's internal purposes, but they are not sufficient to inform companies of which activities, programs, or contracts will be subject to the demands of Level 3.

Satisfaction of Level 3 security requirements is substantially more demanding and expensive. Companies need sufficient time to comply, and that time need translates to early notice of whether Level 3 may apply and when it must be achieved. DoD also should be more accommodating on the time permitted to accomplish Level 3, as certain requirements can be both expensive and require lengthy periods of time to accomplish.

Our members have other concerns about Level 3:

- **Flow-downs**. If a higher tier contractor requires a Level 3 certification, that should not require necessarily that all lower tier participants in the supply chain meet the same requirement. This point should be made explicit. DoD should grant to prime contractors the authority to determine which supply chain participants must meet Level 3 and to implement measures, such as secure enclaves, that will limit the number of lower tier companies obligated to meet Level 3.

- **Certification assessments for Level 3 are to be performed by DIBCAC rather than C3PAOs**. Although DIBCAC has been expanding its personnel, DoD should act to ensure that there are sufficient DIBCAC assessors, qualified to perform Level 3 assessments. Understanding that NIST SP 800-172 and -172A will apply, DoD should improve communications to contractors about how those assessment will be conducted.

- **Credit for satisfaction of Level 3.** DoD also should clarify whether companies that already have satisfied a DIBCAC assessment, or a JSV assessment, are "credited" towards satisfaction of Level 3 requirements should they apply.

4. Program Scheduling and Phased Approach

The Proposed Rule at §1703(d), describes the "phased approach" that DoD intends for the inclusion of CMMC requirements in solicitations and contracts. We see several areas for improvement. First, the scheduling may be too tight, overall. Phase 1 should begin 60 days after the effective date of the CMMC revision to the DFARS, not immediately. Phase 2 is to begin six months following the start date of Phase 1, and in Phase 2, "DoD intends to include CMMC Level 2 Certification Assess all for [sic] applicable DoD solicitations and contracts as a condition of contract award." Considering the number of qualified assessors likely to be available, and the continuing uncertainties as to what external services will be useable, and how they will be assessed or validated, this timing is too fast. Phase 2 should not start for at least a year after the start date of Phase 1, and later Phases should be adjusted accordingly.

In addition, DoD should provide six months of advance notice of requirements, programs, activities, and contracts where it expects to impose a Level 2 or Level 3 certification assessment requirement in advance of the date that the requirements appear in solicitations, option renewals, or other contract terms. Doing so will help many companies manage the costs and other obstacles both to achieving security and to getting necessary assessments. Publishing such advance notice should be accompanied by

opportunity for companies affected, at all levels of the supply chain, to contact the relevant prime, or Contracting Officer, or Requiring Activity, if they have a case to make for relief from or adjustment to when CMMC requirements will be imposed.[10]

5. Affirmations

Affirmations are required annually for each of Levels 1, 2, and 3. *See* Proposed Rule §§ 170.15(a)(2), 170.16(a)(2), 170.18(a)(2). These apply to affirmations for self-assessment, for Level 1, where permitted for Level 2, and after certification assessments, for Level 2 and Level 3. *See also* Proposed Rule § 170.22. The "affirming official" is to be an organization's "senior official who is responsible for ensuring … compliance with CMMC Program requirements." *Id*.

Per Proposed Rule § 170.22(a)(2), the affirming official is to submit a "CMMC affirmation attesting to continuing compliance with all CMMC Level 2 requirements." Similar language is present for Levels 1 and 2. From a standpoint of business operations, over the period that a CMMC certification is valid, it is highly likely that there will be organization changes and/or the introduction of new security methods. DoD should clarify that organizations may obtain a limited review from C3PAOs of such changes in support of the affirmations that are required. DoD, or the Accreditation Body, also may wish to clarify what supporting evidence is required for annual affirmations.

DoD should reconsider the present requirement of annual affirmation of CMMC compliance from a senior official of companies subject to Level 1 (assuming it remains in the CMMC program). This requirement is an unnecessary, additional certification, considering the purposes and operations of the federal government's System for Award Management ("SAM"), which achieves administrative efficiency by centralizing the submission of reps and certs. By adding the Level 1 certification to the annual SAM

---

[10] This approach will allow contractors to prepare should DoD take advantage of the provisions allowing it the discretion to (1) include CMMC Level 2 Certification Assessment in place of CMMC Level 2 Self-Assessment in Phase 1 and (2) include CMMC Level 3 Certification Assessment in Phase 2. If DoD does not implement the advance notice approach described above, DoD should strike the language in § 170.3 (Applicability) and elsewhere that allows DoD this discretion. To allow contractors sufficient time to plan and prepare, phases should be clear and not subject to undefined discretion.

requirements, DoD can get sufficient affirmation, and contractors already are required to review and confirm annually SAM certifications.

6. International Suppliers

The Proposed Rule recognizes that there is no "general prohibition of foreign dissemination of CUI," 88 Fed. Reg. 89067, but the Department offers no relief from longstanding concerns that reconciling the requirements and process of CMMC to international suppliers to DoD and foreign partners of U.S. defense suppliers.[11] We believe this position is non-responsive to the known, actual problem of respecting sovereign laws and limitations on access to or assessment of non-U.S. defense suppliers, with the many formalities of the CMMC framework which clearly focus upon U.S. suppliers. This approach is short-sighted and contrary to many contemporary U.S. national security initiatives which emphasize the proposition of "common defense" and that seek to promote appropriate co-dependence upon and cooperation among an international community of defense suppliers. We strongly recommend that DoD establish a process within the final version of the Proposed 32 CFR CMMC Rule, with accompanying DoD resources, so that actual issues can be raised to DoD officials and resolved. Although country-to-country agreements are best, these can prove difficult and slow to accomplish, and there are gaps in present country coverage. It is in DoD's interest, as well as that of the many international participants in its supply chain, to allow for case-by-case review of actual problems and determination of practical, sufficient solutions.

7. Security Protection Assets

The Proposed Rule requires, for Level 2, that "Security Protection Assets" be documented in the assets inventory, in the System Security Plan, in the network diagram of the CMMC Assessment Scope, and that the OSA or OSC prepare for these to be assessed against CMMC security requirements. The "CMMC Assessment Requirement" for Security Protection Assets is: "Assess against CMMC security requirements." Proposed Rule, Table 1 to §170.19(c)(1). Security Protection Assets ("SPA") are defined as: "Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope, **irrespective of whether or not these assets process, store, or transmit CUI**." *Id.* (emphasis added).

---

[11] Responding to a question on this subject, the Proposed Rule answers that "Contractors are required to comply with all terms and conditions of the contract, to include terms and conditions relating to cybersecurity protections and assessments." 88 Fed. Reg. 89068.

It is curious that the CMMC Rule, which at its core is to protect the confidentiality of CUI, here requires information generated by private sector actors, in providing security protection services, that is *not* CUI – since DoD did not generate, or provide, or designate such information as CUI. Nor does SPA data fit any potentially relevant definition in the CUI Rule, 32 CFR Part 2002, even assuming that, somehow, it applies to this private information.

Second, it seems anomalous for a Rule that is to protect the Confidentiality of CUI, that the assessment requirement applies even where such assets do not "process, store, or transmit CUI."[12]

DoD should not extend CMMC Level 2 assessment requirements to SPA data. Initially, the definition in the Proposed Rule is insufficient to distinguish among the many forms such information may take, or to recognize the different security issues or risks presented. Second, the entities that generate SPA data, MSSPs, for example, typically are not under a DoD contract that imposes upon them any of the -7012 DFARS or CMMC requirements. Clients may lack a legal basis to insist that these SPA service providers must deliver such information or must conform to CMMC Level 2. The same question may be raised as to whether DoD has the legal authority to reach beyond CUI to SPA information.

We recognize that there are security implications to such assets and corresponding data, and we appreciate there are reasons to protect it, but they do not translate to a sound legal or regulatory basis to insist that individual OSAs and OSCs require that their SPA service providers submit to assessment and pass CMMC Level 2 requirements.

Instead, DoD should consider allowing contractors to manage the security of such assets using risk-based security policies, procedures, and practices, as it does for "Specialized Assets." DoD could authorize assessors to review the adequacy of the contractor's risk assessment and documentation of its risk-based actions, as concern SPAs, and confirm that the contractor's actions are in accord with such assessment and

---

[12] DFARS 252.204-7012 defines a "Covered contractor information system" as one that "processes, stores, or transmits covered defense information." "Covered Defense Information" is defined to mean both controlled technical information "or other information" as described in the Controlled Unclassified Information (CUI) Registry.

documentation. Such an approach would be a welcome "light touch" on assessment and burden, and it is what the Proposed Rule affords to Contractor Risk Managed Assets.[13]

8. Definitions and Implementation

DoD should consider the additional points below relating to definitions related to the CMMC program in the proposed rule and implementation of the program.

- Note while "Enterprise" is defined, it is not used in the proposed rule.

- DoD should consider updating the definition for IoT to include the concept that the exchange of data and information between devices occurs over the internet. See proposed revision: "*Internet of Things (IoT)* means the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information [over the internet]."

- Definition of Subcontractor - The DOD should consider updating the definition of Subcontractor and instead rely on DFARS case 2023-D022 to provide a definition, as contemplated in November 2023 in the final rule for DFARS Case 2017-D010.

- DoD should consider establishing a repository for companies to be able to check and confirm attestation and certification status for DoD contractors and subcontractors, as well as FedRAMP equivalency status for CSPs, where required, and ESPs, if required.

- DoD should make clear to contractors how NIST 800-171 Rev 3 will be incorporated into the CMMC program, and provide sufficient time

[13] Relatedly, DoD should consider updating the definitions for "CUI Assets" and "Out-of-Scope Assets" so it is clear CUI Assets are those that do or are intended to process, store, or transmit CUI (we suggest DoD eliminate within the definition that they "can" process CUI); and Out-Of-Scope Assets should be defined as those that do not and are not intended to process, store, or transmit CUI (not necessarily that they "cannot").

for such incorporation, when it is finalized and released.[14] Questions remain regarding how, when revisions to Rev 2 are made or when Rev 3 is released, will such changes affect existing certifications, self-assessments, and/or annual attestations. Similarly, substantial effort will be needed to update and augment the training and accreditation it provides, and supporting documentation, to reflect Rev 3.

C. CONCLUSION

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@thecgp.org or 202-331-0975.

Sincerely,

Roger Waldron
President

[14] The Proposed Rule references SP 800-171 Rev 2 throughout and treats it as the baseline for the CMMC framework and program. Yet, NIST is completing Rev 3 and its companion assessment update. Rev 3 is expected to have substantial changes that will impact the ability and cost of contractors and subcontractors to comply with CMMC. (One example is split tunneling, which is prohibited in Rev 2 but not in Rev 3.) Some of the differences have important operation and technical effects upon companies. Further, Rev 3 expressly is intended to reflect the updated security practices of NIST SP 800-53 Rev 5, and so it is more current and expert guidance. We appreciate that DoD must manage the transition to SP 800-171 Rev 2. We recommend, however, that DoD expressly permit OSAs and OSCs to adopt Rev 3 ahead of when Rev 3 is generally required, and that DIBCAC establish a mapping from Rev 3 back to Rev 2 to guide assessments in such situations.