# Comments of The Coalition for Government Procurement

*By email to* osd.dfars@mail.mil

Ms. Leslie Beavers
Chief Information Officer (Acting)
Office of the Chief Information Officer
Department of Defense
Washington, DC 20301

Re: **Docket DARS-2020-0034**
**RIN 0750-AK81**
**DFARS Case 2019-D041**
**Assessing Contractor Implementation of Cybersecurity Requirements**
**Proposed Rule August 15, 2024**

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.

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 340 members, approximately 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 Program, generally. We previously submitted comments to the 32 CFR Part 170 CMMC proposed rule, as was published on Dec. 26, 2023, at 88 Fed. Reg. 89058. Here, we submit comments to the 48 CFR CMMC proposed rule, 89 Fed. Reg. 66327 (the "48 CFR Proposed Rule"). As discussed more fully

below, however, the Coalition recommends that certain provisions of the 48 CFR Proposed Rule be revised and clarified.

## Implementation Recommendations:

1. Protect Prime Contractors Against Unknowable Risks of Supplier Compliance

This comment concerns proposed DFARS 204.7503. Prime contractors ("Primes") cannot access the Supplier Performance Risk System ("SPRS") and the 48 CFR Proposed Rule provides no means by which Primes can validate the security status, including CMMC compliance, of their subcontractors. If the Government cannot make such information available to Primes (or other higher tier contractors), the regulations should explicitly state that the Government will allow Primes to rely on the representations and certifications of their subcontractors as it relates to CMMC 2.0 level status within SPRS. Primes should not be at risk of penalties for misrepresentations or misstatements by subcontractors regarding CMMC status or certification. This DFARS Part should explicitly state that Primes will not be rendered ineligible for award if the DoD concludes that a subcontractor does not have a timely or sufficient certification status in SPRS. Instead, a Contracting Officer ("CO") should alert the prime contractor of the issue and allow such matters to be dealt with after award of the prime contract. Once a prime contractor is informed of a problem with one of its suppliers, it should not make a subcontract award to that subcontractor until the prime contractor is satisfied there has been successful resolution or mitigation.

2. Improved Flow Down Instruction

The 48 CFR Proposed Rule should be improved and clarified so that Defense Industrial Base ("DIB") suppliers better understand what is expected of them in requirements to flow down CMMC obligations to their suppliers. The 48 CFR Proposed Rule states:

> During the phase-in period, when there is a requirement in the contract for CMMC, CMMC certification requirements must be flowed down to subcontractors at all tiers, when the subcontractor will process, store, or transmit Federal contract information (FCI) or CUI, based on the sensitivity of the unclassified information flowed down to each of the subcontractors …

89 Fed. Reg. at 66328. Many contractors need guidance on DoD's expectations for flowing CMMC certification requirements to their suppliers. The actual risk of information or

information system compromise, varies enormously among contractors and is highly dependent upon the context of the information shared and the scope of work assigned to individual suppliers. It simply is incorrect to presume that the security risks are equivalent for any subcontractor that receives any form of information designated as Controlled Unclassified Information ("CUI"). First, not all of the types of CUI established in the National Archives and Records Administration ("NARA") CUI Registry have the same importance of potential impact to DoD, in the event of compromise, as to others. Not all suppliers receive the same volume of information, or work on programs with the same implications for national security or receive or use data exposed to equivalent third-party threats. These conditions call for DoD to develop a more nuanced approach to flow down, so that CMMC demands imposed upon the supply chain have proportionality to the risks present at each supplier.

Relatedly, the 48 CFR Proposed Rule fails to provide much guidance on what means are available to higher tier contractors to verify cyber compliance prior to awarding work to subcontractors. Primes need better guidance on how to determine flow down requirements and how to validate the security of their suppliers.

3. <u>Confer Discretion to Decide When to Impose CMMC Requirements Within the 4-Phase Implementation</u>

The now final 32 CFR Part 170 established a 4-Phase Implementation Plan. It's unclear if a Requiring Activity ("RA"), or CO, has the discretion to make different decisions on which programs or solicitations to place within the phases. Does a RA or CO have the authority to accelerate or delaying the timelines for programs or contracts under their authority? We suggest DoD confirm that the RA or CO, as applicable, can make decisions when, within the 4-Phase timeline, they invoke CMMC contract requirements. This may be necessitated by a variety of external circumstances, such as whether a Certified Third-Party Assessor Organization ("C3PAO") is available at the time, and the backlog or scheduling situation for assessments. For reference, the now final 32 CFR Part 170 provided that Phase 2 would require Level 2 Certification by a C3PAO only after Phase 1 has been in place for one calendar year. Given the presently small number of C3PAOs and the large volume of contractors subject to Level 2 requirements, the proposed 204.7503 should be revised to make it clear that RAs and COs cannot accelerate that timeline <u>and</u> have the discretion to adjust the timing of when CMMC-specific requirements must be satisfied. COs should be authorized to consider information from contractors regarding their readiness. Informal means should be permitted so that COs can review readiness and regulatory timing with potentially affected suppliers.

4. Authorize Contracting Officers to Decide Upon CMMC Level and Clarify How the Levels Will Be Set

The 48 CFR Proposed Rule, at DFARS 252.204-7021(b)(1)(i), calls upon the CO to "fill in the required CMMC level." Proposed clause 242.204-7YYYY provides for notification to suppliers of the required certification level. The 48 CFR final rule should provide further clarity on the factors to consider in setting the CMMC level and accommodate contractor participation. At present, it is unclear how the "correct" level is to be determined. This leaves DIB partners in the dark on decisions that could affect greatly the time available, or even the feasibility, of meeting CMMC security requirements. DoD also should consider changing the rule to enable COs to make inquiries of contractors, and have consultations, before the CO sets the CMMC level. Because a CO may set a CMMC level that does not reflect the actual possession or use of information by a supplier, or the level or risk involved, it is advisable for the CO to be authorized to conduct fact-finding as needed before the CMMC level is set. We therefore would recommend that DoD clearly outline and publish the methodology for determining CMMC levels, making further changes as outlined above. Consultation with potentially affected suppliers could improve the outcome.

5. Include Flexibility in Administration to Avoid "Knock-on" Exclusion Effects

The Department should recognize the risks to supply chain composition and continuity of supply that may follow implementation of CMMC requirements to programs, solicitations, and contracts. The Coalition fully supports CMMC's objective that DIB companies improve their ability to protect the confidentiality of CUI. There will be situations, however, where CMMC obligations will knock out critical suppliers in a program, weapon system, or sustainment supply chain. Such "knock-on" effects could do harm to warfighters that are disproportionate to the benefits received by eliminating less secure participants from the DIB. This is why it is so important to build in flexibility in the administration of the CMMC contract clause requirements. The practical impacts of CMMC will depend upon the CMMC Level specified, whether a certification assessment is required, and when within the 4-Phase implementation program solicitations incorporate the clause at DFARS 252.204-7021. It will greatly benefit the Department for it to authorize its RAs and COs to make risk-informed decisions on these variables. We think it important to provide for relief from CMMC demands in exceptional circumstances, so that this regulation does not prove disadvantageous to the programs, systems, and capabilities that it is intended to protect.

6. Clarify Treatment of Assessment Artifacts

DFARS clause 252.204-7021 should state that the Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC") may assess or re-assess artifacts that are part of the High Confidence Assessments (Level 2 or Level 3). Re-assessed artifacts that require remediation will be assigned a 6-month Plans of Action and Milestones ("POA&M.") Where DIBCAC has performed a High Assurance assessment, it should be accepted without re-adjudication by other DoD components.

7. Provide Formal Waiver Procedures

The 48 CFR Proposed Rule should create formal waiver procedures. In the now final 32 CFR CMMC Rule, DoD advised:

> Once applicable to a solicitation, there is no process for OSA's to seek waivers of CMMC requirements from the DoD CIO. In accordance with § 170.5(d), a limited waiver authority is provided to the Acquisition Executive with acquisition oversight for the program in question. These officials may issue supplemental guidance dictating specific coordination requirements for waiver requests. Recommended administrative changes have been incorporated into § 170.5(d) to add clarity.

89 Fed. Reg. at 83114. This is not sufficient. In Table 8 to the now final 32 CFR CMMC Rule, DoD estimated there would be 76,598 entities requiring a Level 2 certification assessment, and 4,000 entities permitted a Level 2 self-assessment, over the phase-in period. Another 1,487 companies are expected to satisfy Level 3 certification. 89 Fed. Reg. at 83178. It will not happen that Level 2 or Level 3 CMMC obligations will be achievable by the tens of thousands of companies without numerous instances where one or more of the SP 800-171 controls cannot be satisfied, where certain SP 800-171A assessment objectives cannot be met, and where DoD will be confronted with arguments that "compensating controls" are sufficient and that "enduring exceptions" should be accepted. Because of the high bar set for POA&Ms (excluding all "high point" items under the DoD Assessment Methodology and requiring an 80% minimum score for all assessed items), it is a certainty that many valued contractors will experience compliance glitches, shortfalls, or other problems, as would "fail" the CMMC assessment requirements and exclude them from new or extended DoD supply contracts. Such issues will affect contractors of all sizes, including many who are small businesses, and some who are COTS and commercial suppliers, and the problem will be spread across all facets of DoD acquisition and supply.

Provisions should be added to the 48 CFR Proposed Rule to establish the process for waivers and the considerations used by decision authorities. The authority should include but not be limited to individual contract actions, because some companies will present problems that cut across all DoD contracts held by their enterprise. Thus, the waiver authority should encompass contractors, business segments, programs, as well as contracts and other cost objectives. Levels of higher authorization should be articulated depending upon the breadth, significance, or duration of the waiver. Within the Military Departments, approval by the Head of Contracting Activity likely should be expected. However, where waiver serves the national interest, the authority of Service Secretaries, and senior DoD officials (e.g., SecDef, DepSecDef, and USD/A&S) should be specified.

Some clarity on waivers can and should be specified in the final 48 CFR or 32 CFR CMMC Rules. The Coalition recognizes that full articulation of waiver authority, process, and guidelines could require a separate rulemaking beyond the pending 32 CFR and 48 CFR rules. The Coalition strongly urges that DoD's CMMC leadership to include near-term waiver provisions and start on rulemaking for broader purposes. In the prospective waiver rules, we urge DoD to incorporate risk assessment and outcome comparison into the waiver decisions.

## Notification Recommendations:

1. Reporting "Material Adverse Changes" Rather Than "Lapses" in Information Security

The 48 CFR Proposed Rule, at 252.204-7021(b)(4), would require contractors to notify the CO within 72 hours when there "are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract." The Coalition concludes that this requirement is unclear, and overbroad, as well as burdensome. The operative term, "any lapses," is ambiguous, at best, and will be very difficult for anyone to implement or administer. Moreover, the "any lapses" notification is an unnecessary addition to existing reports required for a cyber incident. While it will produce continuing costs to contractors, and add to the workload of DoD personnel, we do not see proportionate security benefits.

Yet, the Coalition understands and agrees that DoD should be informed where the security of a contractor changes in a way that affects the assurance that the Department has in doing continued business with that contractor. We therefore recommend that this clause be changed to require not a notification of "lapses" but where there is a "material adverse change" in information security or status of a CMMC certificate or self-assessment status. While there is room to debate what constitutes a "material adverse change," this approach is familiar to

business enterprises and it sets a higher bar, for notification to DoD, than does the present "lapses" language.

2. Consider Government-wide Initiatives to "Harmonize and Streamline" Reporting

To require notification over an undefined "lapse in information security" seems contrary to the DoD's and Congress' stated desire to harmonize and streamline reporting and notification requirements under myriads of cybersecurity clauses being issued by various federal agencies. Currently, DFARS 252.204-7012(c) includes a requirement to report to the DIBNET within 72 hours of a "cyber incident." We recommend that DoD rely upon this current DFARS provision as the authoritative guidance for reporting of cyber incidents. Several members of the Coalition urge that DoD go further and remove from the 48 CFR Proposed Rule the requirement for contractors to report lapses in information security in this clause. Their position is that the new requirement adds unnecessary steps that should be handled using the existing DIBNET portal and SPRS systems. They note that the SPRS system allows Contracting Officers to check and monitor for supplier compliance in a "one-stop-shop," suggesting little incremental benefit to additional reporting. The Coalition is willing to support new reporting of "material adverse changes," as explained above, but believes that DoD should emphasize leverage of the systems it already has for visibility into contractor security over time.

3. Reconsider Notification to Contracting Officers

As noted, the 48 CFR Proposed Rule, at 252.204-7021(b)(4), introduces a requirement to notify the Contracting Officer within 72 hours when there are any "lapses" in information security or changes in the CMMC status. Apart from our other reservations, we question whether it is prudent to require such notifications to Contracting Officers. Doing so invites potentially numerous notifications, if a DIB supplier has multiple DoD contracts subject to CMMC. Where multiple COs receive such notices, the likelihood is high that there will be confusion, uncertainty, and inconsistency in such responses as individual COs make to these notifications. This serves the interest of no one. The better way to handle notifications – of "material adverse changes" as we urge – is for the notifications to go to the existing DIBNET Portal, using SPRS systems as employed today. Once eMASS systems come to host CMMC assessment results, it could be appropriate for the notice to go to that system as well. Many officials with the Department, including Contracting Officers, have access to these DoD-enterprise systems. This is a much better outcome than demanding a flurry of notices to individual COs when the disposition or value of such notices is no better than conjectural. Notification via the DIBNET

portal is more efficient, sufficient for DoD purposes, while consuming less time and resources of DIB companies.

The 48 CFR Proposed Rule requires contractors to "report to the [CO] of any changes in the list of DoD UIDs applicable to each of the contractor information systems that process, store, or transmit FCI or CUI during contract performance and to provide the corresponding DoD UIDs for those contractor information systems." 89 Fed. Reg. at 66329; *see* proposed DFAR 252.204-7021(c)(3). This is an overbroad requirement because networks are constantly changed and maintained. They are not static, and, in fact, to sustain security over time, in an evolving threat environment, virtually *requires* adjustments and improvements – all of which, under the proposed DFARS, would represent reportable "changes." As presently drafted, the requirement is against DoD's interest as, arguably, it would motivate companies not to improve (and therefore change) their information systems, in order to avoid reporting. Accordingly, if this language is retained, CGP recommends it be revised to require notification only when changes have a material, adverse impact upon the contractor's compliance with the specified CMMC level.

## COTS and Commercial Recommendations

1. Clarification of COTS Seller Definition

The Coalition seeks clarification of the commercially available off-the-shelf ("COTS") items exclusion in the 48 CFR Proposed Rule. The preamble to the Rule states that it will not apply to COTs which are defined at FAR 2.101. *See* 89 Fed. Reg. at 66238. A COTS item, according to FAR 2.101, is defined as an item that is "sold in substantial quantities in the commercial marketplace." A COTS product is one that has been sold, leased, or licensed to the general public. One Coalition member asks whether the COTS exclusion is limited to items that individual companies have sold or offered to the commercial marketplace? Or, they ask, is the intent that the COTS exclusion applies to products that are generally sold in the commercial marketplace by anyone? We seek clarification. We assume that the answer to the former question is that a COTS item is one that any seller, rather than an individual seller, offers to the commercial marketplace in substantial quantities. This company also inquires whether the COTS exclusion applies to services directly related to a commercial product such as warranty, installation, or training? The 48 CFR Proposed Rule should be clarified so that such ancillary services are plainly subject to the COTS exclusion.

2. Protection of COTS Sellers Against Misapplication of CMMC Requirements

A member of the Coalition that is a furniture manufacturer observes is considered selling COTS items. CMMC should not apply to it. However, on certain large government business opportunities, this company has been asked to sign off on receipt of CUI and to application of DFARS cyber requirements in order to gain access to floorplans relevant to the supply of COTS furniture. This manufacturer has declined to participate in those solicitations because it does not intend to be certified for CMMC that should not apply. We urge clarification of the 48 CFR Proposed Rule to prevent Contracting Officers (or Prime Contractors) from unnecessary flow down of CMMC requirements to COTS providers such as this company. Alternatively, a means should be provided for COTS providers to demonstrate to Contracting Officers (or Primes) that flow down is not appropriate. As concerns COTS suppliers, DoD should understand that the CMMC rules, when applied unnecessarily, presents difficult administration and governance problems for companies with a national spread and multiple small offices and locations (office/factory/storage/shipping).

## Other Recommended Clarification

1. DoD Unique Identifier

The 48 CFR Proposed Rule adds a definition, at 204.7501, of "DoD unique identifier" (or "DoD UID"), which means "an alpha-numeric string of ten characters assigned within the Supplier Performance Risk System to each contractor assessment with the first two characters indicating the confidence level of the assessment." Some members of the Coalition are uncertain of the relationship between the DoD UID and CAGE Codes, and they also ask for clarification of how the DoD UIDs will be used in the CMMC framework. Particular clarification is requested with regard to how contractors may define "contractor information system" for purposes of generating a DoD UID(s) for systems that process, store, or transmit only FCI. Some large commercial companies potentially have FCI in hundreds of systems depending on how "system" is defined and the exercise of inputting information and providing an affirmation for each will be a large undertaking. It is recommended that DoD allow for a company-wide assessment and affirmation for Level 1 and, if not, allow an extended implementation time from the date of the final rule. This is consistent with current CMMC 2.0 Level 1 scoping guidance, which provides, "[b]ecause FCI is a broad category of information, the contractor will likely focus the self-assessment on their entire environment." We think DoD should improve its explanation and take care not to introduce, by use of DoD UIDs, another unnecessary layer of complexity with uncertain benefit.

2. Contractor Information Systems

The 48 CFR Proposed Rule, at 204.7503, and in the contract clauses at 252.204-7021 and 252.204-7YYY, uses the term "contractor information systems." The underlying DFARS clause 252.204-7012 refers to "covered contractor information systems" in seven (7) places but does not use the term "contractor information systems" without the "covered" adjective. Coalition members are uncertain of the significance of the different phrasing, and raise concerns that usage of the different phrase in the 48 CFR Proposed Rule will broaden the scope of applicability to information systems which, because they are not "covered," are unrelated to CUI and FCI.

3. Security Changes

The 48 CFR Proposed Rule references, 89 Fed. Reg. at 66329, a requirement that contractors complete and maintain, on an annual basis, "or when security changes occur," the affirmation of continuous compliance with security requirements. This term is not used in the operative contract clauses in the 48 CFR Proposed Rule and has no corresponding utilization in the now final 32 CFR Rule. The term "security changes" is not self-defining, and the 48 CFR Proposed Rule does not provide a sufficient, definition, metric, or framework to determine what constitutes such a "security change" as would necessitate reporting. The Coalition believes that "security changes," unless more clearly and narrowly defined, will create confusion and potentially cause unnecessary increased work that presents little to no value to DIB and DoD. A better definition will limit obligations that flow from "security changes" to those that have importance to and support DoD's mission.

The same objection and recommendation apply to the use of "changes" in the proposed DFARS 252.204-7021. There, at 252.204-7021(c)(3), contractors are to report to the CO "any changes to the list of DoD UIDs applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract." Changes to information systems occur constantly and nothing in the fact or presence of a change necessarily suggests or implies any adverse consequence to the security that DoD seeks. Previously, we've observed that DoD should leverage the existing reporting requirements of DFARS 252.204-7012 (c). If DoD feels compelled to add further notification obligations, the reporting should be limited to significant changes of that adversely affect DoD's mission.

4. Separate CMMC Security Levels; Enclaves

The 48 CFR Proposed Rule has the following language at 252.204-7021(b):

> (b) *Requirements*. The Contractor shall –
> …
> (2) Maintain the CMMC level required by this contract for the duration of the contract for all information systems, used in performance of the contract, that process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI);
> (3) Only process, store, or transmit data on information systems that have a CMMC certificate or CMMC self-assessment at the CMMC level required by the contract, or higher;

There are several significant problems with this language. First, the language could be interpreted to mean that where a contract requires a particular CMMC level for some information, e.g., Level 2 for CUI, the same level must be maintained for all information systems of that contractor, even those that deal only with FCI but not CUI. This is contrary to a central principal of CMMC, namely, that companies can establish enclaves within their information systems so that FCI can be maintained at one, lesser level of security, while CUI is maintained at a higher level. The proposition applies equally to situations where a DoD customer requires that CUI be protected at CMMC Level 3. It is important that this clause not be construed to mean that if *some* information is subject to Level 3, then all FCI and CUI on the same information system must be protected at that higher level. Contractors are required to provide the DoD UID(s) "applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract." Proposed DFAR 204.7503(b)(2). The 48 CFR Proposed Rule should be made clear that a location may process FCI or CUI at the different levels of security required by CMMC Levels 1, 2 and 3 – and not all at the highest level as may apply.

5. Senior Company Official

The 48 CFR Proposed Rule states that an affirmation of continuous compliance, where required, is made by a "senior company official." 89 Fed. Reg. at 66329, 66333, 66335. The same term is *not* used in the now final 32 CFR CMMC Rule, as it uses the term "Affirming Official." Neither term is adequately defined in either the final 32 CFR or 48 CFR Proposed Rule. Coalition members observe that the "affirmation" by a company official is an act that has potential compliance and legal consequences. It is important to understand the level of official, or the nature of her or his duties, that DoD expects of a "senior" person making the affirmations. This should be made clear in the final Rule.

6. Definition of FCI

The 48 CFR Proposed Rule relies on the definition of FCI from 48 CFR 4.1901. An original definition of FCI, unique to CMMC, is requested. This definition should clarify certain terms (such as "not intended for public release" and "simple transactional information") and provide that FCI under DoD contracts subject to CMMC will be marked or otherwise identified. DoD should also consider implications of the Freedom of Information Act ("FOIA") on the FCI definition. Information that can be obtained through a FOIA request becomes public information. It would be helpful to have more clarity on this point as information that may be made public through a FOIA request does not appear to meet the definition of FCI. Adopting the current definition of FCI may lead to confusion and a more broad application of CMMC than is necessary.

## Observations Regarding the Structure/Strategy of the CMMC Program

1. Affirmation Requirements

Some members of the Coalition question the value of the affirmation requirements. CMMC introduces a requirement that tens of thousands of companies, at Level 2 or 3, must pass independent third-party assessments in order to receive compliance certifications upon which their eligibility for future DoD business depends. This is the strength of the CMMC program. Adding affirmation obligations, in the view of these companies, adds little value to the process, while creating additional cost and work. The affirmation requirements also introduces further legal and compliance uncertainty and add to the compliance burden with uncertain value gained.

2. Regulatory Harmonization

The CMMC rules create a very detailed and complex set of requirements that apply just to DoD contractors. Many of these contractors also perform work for civilian agencies, and many are subject to a variety of federal cybersecurity and incident reporting regimes. Already, there is widespread concern about the increasing costs of cyber compliance where so many different regulations apply. Wherever possible, the 48 CFR Proposed Rule should be updated to achieve better reciprocity across existing regimes. Regulatory harmonization is needed not only within DRARS, but also across the federal technology ecosystem. The 48 CFR Proposed Rule should explicitly enable harmonization and formalize available reciprocity with other IT security frameworks. FedRAMP is an important example. The cloud security requirements of FedRAMP, as apply under FISMA to federal agencies and departments, need not and should not apply

equally to any form of cloud or external cloud-based service as DIB contractors may use in their business and to operate and secure their information systems. Before transposing one security regime, like FedRAMP, to a different domain than that for which it was designed and intended, DoD should carefully determine what is necessary, cost-effective, and produces a sufficient outcome in light of informed risk management assessment.

3. Sufficiency

The now final 32 CFR CMMC regulations and 48 CFR Proposed Rule are lengthy and complex. They are difficult for most companies to understand and even dedicated "experts" often disagree as to meaning or application of the many rules and requirements. Furthermore, CMMC will require tens of thousands of DIB suppliers to satisfy demanding NIST-based cyber requirements and to pass third party assessments as a condition to continued business with DoD. For all the good intentions of the CMMC program, and with due recognition of the threat conditions that call for increased information security, DoD must take an active role to manage CMMC implementation so that the program both succeeds to improve information security and retains full and vibrant participation, by large and small contractors alike, and by legacy as well as innovative sources. This balance will not be found if each of the many obligations of CMMC rules are interpreted and applied to require the "most possible" rather than what is "sufficient" for acceptance.

DoD must act to manage, oversee, administer, and guide CMMC implementation. Too many businesses today, especially smaller businesses, have trouble making the "business case close" for the costs of CMMC compliance versus their DoD sales revenues and returns on investment. DoD cannot be cavalier to these widespread concerns. The Department can and should act decisively to manage the regulatory burden and costs, so that CMMC is accomplished without excessive costs of compliance and the risks of attrition in in the DIB industrial base and resulting supply chain disruption.

## Health Care Issues

The Coalition includes among its members companies who build and sell COTS medical devices. One of these members raises a significant concern about the disparities in how the Food and Drug Administration ("FDA") qualifies the safety of such devices and mentions that DFARS requirements can be at odds with what the FDA requires. Medical device companies need greater clarity on how CMMC requirements will apply to them. Considering the extent and intensity of FDA requirements for device authorization and continuing security, DoD should consider whether it serves a positive or negative purpose to cause medical device makers to

incur additional expense to comply with CMMC requirements. Medical device suppliers are highly regulated by agencies possessed of domain-specific expertise. The FDA should be respected as the authoritative source of medical device cybersecurity requirements. DoD should not interpose obligations, such as CMMC, that conflict or even interfere.

CMMC compliance, if demanded of such device suppliers, imposes non-recurring investment requirements and continuing costs that may produce no more than incidental or collateral security benefits. DoD in fact may injure its own interests if the CMMC demands cause medical device makers to refrain from offering devices into the DoD market, as is a real possibility. The Department's best interest, here, could well be served by forbearance from application to CMMC to commercial medical devices that also can be sold to DoD. This area illustrates the value of having identified, funded, staffed, and authorized CMMC program management resources, within DoD, who can deal sensibly with sector, enterprise, or product-specific problems.

## 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