United States Department of Defense
Defense Acquisition Regulations System
OUSD(A&S) DPC/DARS
Room 3B941, 3060 Defense Pentagon
Washington, DC 20301-3060
Osd.dfars@mail.mil

RE: DFARS Case 2019-D041

Content

Executive Summary

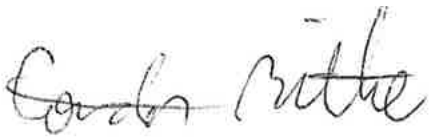
The Information Technology Industry Council (ITI) remains committed to partnering with the U.S. Department of Defense (DoD) to enhance the U.S. national security posture while also maintaining our technological leadership and international competitiveness. In this letter, we offer a set of recommendations to strengthen the implementation of the NIST SP 800-171 assessment requirements and the Cybersecurity Maturity Model Certification (CMMC). On the following pages, we provide specific details why these recommendations are in the best interest of U.S. national security and continued technology leadership.

For the NIST SP 800-171 DoD Assessment Methodology as defined in DFARS 252.204-7019 and -7020, we encourage DoD to include language in the final rule to 1) Define the appropriate boundaries for the self-assessment; 2) Set the parameters of what warrants Medium and High Assessments; 3) Provide additional information on the authorized assessment organizations; 4) Assign clear responsibilities and accountabilities for assessment of subcontractors; 5) Clarify how contracting officers will use the assessment results; and 6) Avoid duplications of the NIST SP 800-171 DoD Assessments with the CMMC requirements upon successful implementation.

For the CMMC requirements per DFARS 252.204-7021, we encourage DoD to include language in the final rule to 1) Ensure CMMC assessment results are safely stored; 2) Allow for flexibility when requiring compliance at time of award; 3) Provide more detail on certification requirements for complex business environments; 4) Clarify the recertification process and allow for timeline flexibility; 5) Provide Department-wide guidance to ensure consistency in CMMC requirements; 6) Expand on reciprocity efforts with other cybersecurity standards; 7) Allow prime contractor flexibility in flow down requirements; 8) Clarify applicability to entities providing Commercially-Available Off-the-Shelf (COTS) Products; 9) Better define the role of CMMC Levels 4 and 5 in the DoD cybersecurity ecosystem; and 10) Ensure an efficient and accountable Accreditation Body that is free from conflicts of interest and appropriately funded to execute its mission.

We appreciate DoD's attention to our recommendations. We hope to work with DoD and other government agencies to fulfill this vision and strengthen the U.S.'s commitment to a secure government and industrial base.

Sincerely,



Gordon Bitko

Senior Vice President of Policy, Public Sector

Information Technology Industry Council (ITI)

I. Preface

The Information Technology Industry Council (ITI) appreciates the opportunity to provide input into DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements. ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader around the globe. ITI's membership is comprised of top innovation companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Many of ITI's members are longstanding partners with the U.S. Department of Defense (DoD), providing innovative products and services intended to help DoD deliver on mission and build up the United States' technological advantage against its adversaries.

U.S. national security depends greatly on U.S. technological leadership. This leadership drives U.S. innovation, job creation, and economic growth. Remaining at the cutting edge of developing and commercializing technologies will solidify the availability of these technologies to the private sector and the defense industrial base (DIB). We share DoD's desire to ensure that U.S. companies remain among the most innovative and competitive in the world. The cycle of private-sector research and development (R&D) efforts— producing market-leading products on a global scale and reinvesting revenues from these products to fund future innovation— is critical.

ITI's members know from first-hand experience the challenging and evolving nature of cyber threats. Cyber-attacks and IP theft pose great risks to DoD, the defense industrial base, and the overall national and economic security of the United States. That is why ITI has provided industry input into DoD's Cybersecurity Maturity Model Certification (CMMC) from the very beginning, holding multiple meetings with DoD personnel throughout 2019 and 2020 and authoring a multi-association letter[1] in March 2020 outlining suggestions for improving the model.

ITI believes that it is important to get this right by developing and implementing those cybersecurity protocols that are necessary, while simultaneously guarding against actions and regulations that do not add security and result in harm to industry's ability to innovate and partner with DoD. In this spirit, we identify below areas in the rule that could benefit from further elaboration and consideration and provide additional suggestions to ensure the CMMC process is fair, efficient, and effective. Our recommendations will ensure that we protect national security without compromising U.S. technological leadership, innovation, or international competitiveness.

[1] https://www.itic.org/policy/CMMCmultiassociation_March26_Final.pdf

II. Department of Defense NIST SP 800-171 Assessment Methodology

We strongly support efforts to improve DIB cybersecurity and agree with the need to assess contractors' compliance with the NIST SP 800-171 standard until CMMC is fully implemented. We appreciate the tiered structure of these NIST SP 800-171 DoD Assessments commensurate with mission criticality and support the decision of awarding contracts based on self-screening with the option for subsequent audits. To ensure a smooth implementation, additional guidance is required on how critical details of the rule will be implemented.

We encourage DoD to include language in the final rule to 1) Define the appropriate boundaries for the self-assessment; 2) Set the parameters of what warrants Medium and High Assessments; 3) Provide additional information on the authorized assessment organizations; 4) Assign clear responsibilities and accountabilities for assessment of subcontractors; 5) Clarify how contracting officers will use the assessment results; and 6) Avoid duplications of the NIST SP 800-171 DoD Assessments with the CMMC requirements upon successful implementation.

General Comments on Assessment Methodology

Relying on a self-assessment marks an effective way to conduct an initial compliance screening of DoD contractors. While all necessary information should be available from the system security plans (SSPs) and plans of action and milestones (POA&Ms), DoD should provide additional guidance on how to determine the appropriate boundaries for documentation of the self-assessment in the Supplier Performance Risk System (SPRS). Besides providing more certainty about the correct scope now, this will also ensure consistency once the NIST SP 800-171 DoD Assessment results are translated into corresponding CMMC requirements.

Similarly, we request the DoD provide clarity around applicability. The rule indicates that a Basic Assessment is required when the clause at DFARS 252.204-7012 is applicable. Since 2015, this threshold has led to confusion and concern throughout the DIB because contracts and contracting officers have not always indicated the presence of CUI or properly marked CUI as required under that rule.

We understand DoD's desire to ensure all contractors' compliance with existing regulations and standards. DoD should continue its contractor audits to enforce a standardized interpretation of NIST SP 800-171 requirements. These audits will be most efficient and least obtrusive when contractors can prepare for them beforehand. Currently, contractors still have an insufficient understanding of the discrete trigger points for the Medium and High Assessments. While the rule discusses the methodology for each assessment and estimates the number of audits that DoD expects to conduct annually, it is silent on what discrete levels of mission criticality warrant a Medium or a High Assessment and who controls the assessment level escalation. We, therefore, encourage DoD to determine clear parameters of what warrants Medium and High Assessments respectively to help contractors prepare for these audits upon contract award,

including the possibility of indicating in a solicitation that award will result in a Medium or High Assessment. Additionally, DoD should include contracting officers in the escalation decision and provide them with appropriate training to identify which contract provisions map to the Basic, Medium, and High Assessments.

Moreover, we encourage DoD to provide additional information on the organizations that will be conducting these assessments. The rule explicitly mentions the Defense Contract Management Agency (DCMA), which makes sense given that they have proven their expertise with the DIBCAC assessments. But the rule also allows other organizations to assess contractors if they are identified by their Department of Defense Activity Address Code. What other DoD or third-party entities will be authorized to perform the NIST SP 800-171 Assessments? If third-party entities are used to perform the NIST SP 800-171 Assessments, will there be a process for avoiding conflicts of interest? Will additional assessors increase the stated capacity of annually performed audits? What are the implications of potential assessment shortages given the cap of 200 and 110 audits for Medium and High Assessments respectively? If there is a need to escalate the assessment level, will the same organization conduct the subsequent assessment and how will DoD handle or consider the associated cost impact in the escalation decision?

Given the high sensitivity of the self-reported data, we appreciate the rule's language to classify the data itself as CUI. Similarly, we strongly support that only Department officials and authorized representatives of the offeror can access the summary level scores and associated information. We encourage the Department to protect this data even further by explicitly stating that at no point in time, may third parties access another entity's summary level scores, including primes and subcontractors.

Finally, according to DFARS clause 252.204-7020 (g), contractors need to flow down the Basic Assessment requirement to all subcontractors. We support the effort to eliminate potential attack vectors by raising the security baseline for all subcontractors. However, there remains confusion around the responsibilities and accountabilities in the enforcement of this clause. What documentation should primes require from subcontractors to attest that they have successfully completed the Basic Assessment? Will subcontractors who do not receive any controlled unclassified information (CUI) need to complete the Basic Assessment? In multi-tiered environments, who will be held accountable for missing or inaccurate self-assessments and who will have the authority to bring contractors into compliance? We encourage the Department to address these questions and require primes to flow down DFARS clause 252.204-7020 (g) only if the prime must supply CUI to the subcontractor to perform the contract and hold each (sub-)contractor accountable only for their own compliance.

Contracting Officers' Use of Assessment Results

While the rule speaks to the methodology and cost for the NIST SP 800-171 assessments, it remains ambiguous on how contracting officers will use these scores. The rule states that

"proper calculation of the score and its submission may well determine whether or not the company is awarded the contract." It is unclear what happens if a company is awarded a contract based on its high self-reported score, but a subsequent Medium or High Assessment finds the score to be lower than initially reported.

Further, the rule does not specify how the summary scores and confidence levels will be weighted and how this will impact future contract awards. For example, will contracting officers be instructed to prefer a lower, government-confirmed score over a higher self-reported one? We would expect a confirmed score to hold more weight than a self-reported one. If true, this would disadvantage those offerors who could not achieve a higher confidence level due to the low number of annual assessments and likely lead to an explosion of disputed assessments.

What is the connection between the rule and the Proposed Rule for the Use of Supplier Performance Risk System (SPRS) Assessment (DFARS Case 2019-D009) published on August 31, 2020? Will the NIST SP 800-171 Assessment scores be used as part of a contracting officer's general responsibility determination (per FAR 9.104-1) or special responsibility determination (per FAR 9.104-2)? Will the scores be an evaluation criterion for all contract awards? If so, will specific requirements be specified in the solicitation?

As one possible way to avoid this confusion, DoD could instruct contracting officers to review the assessment results as part of the general responsibility assessment. This would ensure compliance with NIST SP 800-171 without skewing fair competition.

Transition Period

We greatly appreciate DoD's commitment to eliminating duplicative certifications for contractors. We, therefore, encourage DoD to provide additional guidance on the future of the Medium and High Assessments upon full implementation of the CMMC. The rule justifies the assessments as follows:

> *The NIST SP 800-171 DoD Assessment Methodology provides a means for the Department to assess contractor implementation of these requirements as the Department transitions to full implementation of the CMMC, and a means for companies to self-assess their implementation of the NIST SP 800-171 requirements prior to either a DoD or CMMC assessment.*

Upon full CMMC implementation, certified third party assessment organizations (C3PAOs) will assess and certify contractors' compliance with NIST SP 800-171 as part of CMMC Level 3. Consequently, maintaining the Medium and High Assessments would duplicate this certification, increase compliance costs without a clear benefit, and unnecessarily tie up DoD resources. To adhere to its own stated goal of eliminating duplicative certifications, DoD should abandon the Medium and High Assessments upon full implementation of the CMMC.

Moreover, DoD should clarify how the transition from NIST SP 800-171 DoD Assessments to CMMC will be structured with regards to risk acceptance. The rule explicitly states that POA&Ms will be insufficient to comply with CMMC requirements. At the same time, the rule rightfully acknowledges that problems are inevitable in complex environments. Implemented capabilities may underperform due to a temporary deficiency. For example, critical security patches may not consistently be installed in an organizationally defined period of seven days but may take 20-30 days for subsequent testing.

The DPC standard[2] describing the Assessment methodology accepts POA&Ms as implemented if they are used to fix such a temporary deficiency and further allows for enduring exceptions and CIO waivers. It remains unclear, how C3PAOs will handle these cases once they take over the assessments. The current reading suggests that POA&Ms and exceptions will disqualify contractors for their CMMC certification. We encourage DoD to resolve this issue by distinguishing between the different types of POA&Ms and allowing enduring exceptions, waivers, and POA&Ms for temporary deficiencies in the CMMC requirements.

III. Cybersecurity Maturity Model Certification (CMMC) Requirements

We appreciate the iterative roll-out of the CMMC requirements over a five-year period. This approach provides multiple opportunities to adjust CMMC processes and requirements based on the findings from pilot programs and pathfinders. At the current stage, additional guidance is required on how critical details of the rule will be implemented.

We encourage DoD to include language in the final rule to 1) Ensure CMMC assessment results are safely stored; 2) Allow for flexibility when requiring compliance at time of award; 3) Provide more detail on certification requirements for complex business environments; 4) Clarify the recertification process and allow for timeline flexibility; 5) Provide Department-wide guidance to ensure consistency in CMMC requirements; 6) Expand on reciprocity efforts with other cybersecurity standards; 7) Allow prime contractor flexibility in flow down requirements; 8) Clarify applicability to entities providing commercially Available Off-the-Shelf (COTS) Products; 9) Better define the role of CMMC Levels 4 and 5 in the DoD cybersecurity ecosystem; and 10) Ensure an efficient and accountable Accreditation Body that is free from conflicts of interest and appropriately funded to execute its mission.

Consider simplifying CMMC requirements

The interim final rule explicitly states that it "does not duplicate, overlap, or conflict with any other Federal rules." The CMMC requirements do, however, duplicate NIST SP 800-53 Rev 5 and NIST SP 800-171 requirements, and establish a new framework against which members of the defense industrial base must measure themselves. A more simplified solution would be

[2] https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf

preferred by continuing existing NIST SP 800-171 requirements and control statements, while supplementing via SP 800-53 CMMC Level 4 or Level 5 "Control Overlays" where greater risk exists.

Ensure CMMC Assessment Results are Safely Stored

The rule states that CMMC assessment results (as well as the results of the NIST SP 800-171 Assessments), will be posted in the Supplier Performance Risk System (SPRS) in order to provide DoD Components with visibility to CMMC certifications for DIB contractor networks. While we appreciate that this approach to storing assessment results is intended to reduce cost and burden to DoD and industry, we believe the rule must articulate the steps DoD will take to ensure these results are safely stored and handled. CMMC assessment results will contain very sensitive information about a company's operational practices and security posture, and the impact on contractors if these results were to be exfiltrated would be disastrous, creating a potential target list for malign actors and exposing company information.

We recommend that the final rule lay out a specific process for protecting assessment results once they are posted in SPRS. Among the various steps should be a limitation on who within DoD can view any given company's assessment result. We believe that DoD personnel at the program level should only be authorized to view a company's assessment result if that company has received or is in consideration for an award. DoD should consider striking a balance of not oversharing this information, with the intent of limiting details that could be exfiltrated and uncovered by an adversary. Additionally, we caution against granting prime contractors access to SPRS for the purpose of selecting a compliant subcontractor. Given the vast number of registered DoD prime contractors, allowing every single one of these contractors to access SPRS will create countless new attack vectors for any company featured in the database. It is not necessary to grant prime contractors access to SPRS for verification purposes, since subcontractors will be able to show their certificate from the CMMC Accreditation Body to prove compliance with the required CMMC impact level. In addition to limiting access to SPRS, DoD should consider limiting the distribution of the CMMC certification level achieved by organizations. By limiting awareness of the CMMC certification level obtained by organizations, this will limit public knowledge of which organizations have access to DoD's data. DoD should strongly discourage DIB companies from publicly advertising their achieved CMMC level, as this would provide our adversaries with information that could be used to harm national security.

Allow for Flexibility When Requiring Compliance at Time of Award

ITI supports DoD's requirement for prime contractors to demonstrate CMMC compliance at the time of contract award, rather than at the time of proposal submission. Requiring bidders to demonstrate CMMC compliance when submitting proposals would unnecessarily limit the field of competition to established vendors in the defense industrial base (DIB). In contrast, allowing

prime vendors to demonstrate compliance at award increases opportunities for non-traditional defense contractors to successfully compete on DoD solicitations.

Flexibility should be provided when a company is certified at time of bid submission but a subsequent audit may determine the contractor to be deficient prior to award, and there is insufficient time for the contractor to take remedial action to comply. For example, if an audit result is released the day before award, there may be insufficient time for the contractor to take remedial action. In such a situation, DoD should allow contractors a reasonable amount of time to comply after award but prior to the scheduled beginning of contract performance.

ITI also requests flexibility when applying this requirement to subcontractors, assuming the contract allows for mitigation options regarding access to CUI. For example, if a prime contractor is CMMC-certified at the time of contract award but a subcontractor is not, and if the subcontractor can be appropriately firewalled from accessing CUI until achieving CMMC certification, there should be no barrier to awarding the contract to the prime. If needed, the contract could be awarded with an additional requirement for the prime to prohibit subcontractors' access to CUI until all subcontractors are appropriately certified.

ITI further requests clarification regarding how the government will prioritize scheduling assessments for contractors. Given that contractors must demonstrate CMMC certification (which requires a completed assessment) at the time of award, we are concerned that a delayed assessment due to competing priorities set by DoD or delays caused by the C3PAO could impact a contractor's eligibility for award. For example, if the government prioritizes established DIB contractors or subcontractors for assessments, this could create an unfair competitive advantage for these companies vis-à-vis companies that are new to the DIB and thus lacking a CMMC assessment. If an assessment is delayed based on circumstances outside the contractor's control, we urge DoD to adopt policies and procedures that allow that contractor to nevertheless be considered for award.

Provide More Detail on Certification Requirements for Complex Business Environments

One of ITI's main concerns detailed in our multi-association letter was how certification requirements will apply in the case of complex business environments. CMMC v1.0 provided some technical details on how to operate solutions in a complex environment but did not clearly describe how to define organizational and logical system boundaries in order to determine the appropriate level of CMMC certification. For instance, if a large business has a separate subsidiary or business unit that handles all sensitive information related to DoD contracts, will the whole entity need to be certified if its central systems (H.R., finance, legal, contracts, *etc.*) only handle very basic FCI (for instance, a list of the DoD contracts held by that entity)? A more specific example is that CMMC Levels 4 and 5 require that the contractor operate a Security Operations Center (SOC) that facilitates a 24/7 response capability (control

IR.4.101). It is unclear whether the SOC would need to be dedicated only to the specific business unit handling CUI or whether DoD intends for the SOC to span the whole corporate enterprise.

The Federal Risk and Authorization Management Program (FedRAMP), which is also based on NIST SP 800-171, provides an example of the challenges posed by this lack of elaboration. While the intended controls are ideal, they are not suited to a continuous integration (CI)/continuous delivery (CD) pipeline and rapid updates and deliveries to improve service. Companies often make hundreds of changes per day and the FedRAMP controls do not align well with CI/CD. Boundaries become critical, and more often than not, the U.S. government tends to favor incorporating many subsystems into the boundary or creating duplicative systems to meet the controls, which increases costs significantly. This is an issue for CMMC and FedRAMP alike; most Software-as-a-Service (SaaS) solutions are much more complex than shrink-wrapped COTS which are standalone. Many systems are integrated from proof of value (POV) to acquisition to production deployment, and all of these systems are interconnected. Though the rule notes that contractors will achieve a certain CMMC level either for their entire enterprise network or for certain segments "depending on whether the information to be protected is processed, stored or transmitted," we request that DoD develop a standardized methodology for determining what circumstances would require the whole entity to obtain CMMC certification, and to maximize circumstances under which certification could be limited to a certain network segment or enclave.

Clarify Recertification Process and Allow for Timeline Flexibility

In the modern business environment, contractors must respond to change often and quickly. The decisions made when responding to change are not made in isolation and will likely spillover into (un-)related business units. Some of these changes may warrant a recertification of a contractor's compliance with the CMMC requirements. Currently, the rule does not provide any guidelines on what instances may necessitate a recertification process prior to the certification's expiration date. We understand that this will ultimately have to be a case-by-case decision and we support the government's authority to make that call. Nonetheless, it will be helpful to give contractors a list of potential triggers so they can prepare for and expedite the recertification process.

For example, what will happen if a CMMC-certified contractor takes a majority stake in another company? In this case, we believe the contractor should not be required to recertify unless there are changes to the system architecture. Further, what happens if the acquired entity itself is CMMC certified, but possibly at a different level? Again, we understand that there cannot be a comprehensive list of recertification trigger points but encourage DoD to provide additional guidance so contractors can prepare for recertification early on. Reducing the time that

contractors need to recertify will promote greater diversity of potential bidders in future solicitation processes.

Ultimately, the CMMC assessments conducted by a C3PAO will only capture a company's security posture and operational practices at a static point in time. Given the speed of technological developments and the rapid proliferation of cyber threats, a three-year audit is not the most effective way to ensure network security, especially when measuring an organization's ability to defend itself against advanced persistent threats (APTs). ITI recommends that DoD consider allowing contractors to demonstrate continuous monitoring capabilities for certain controls in lieu of a strict three-year recertification requirement, or to allow for a longer recertification period if a contractor demonstrates these capabilities.

Provide Department-wide Guidance to Ensure Consistency in CMMC Requirements

CMMC represents a major shift in DoD-wide cybersecurity requirements for contractors. Government contracting officers and program officials will be responsible for implementing and enforcing CMMC requirements in all DoD programs. It is imperative that government officials across DoD and the Services receive consistent, adequate training on implementing CMMC requirements. Additionally, DoD must establish a robust audit program for ensuring the successful and consistent implementation of CMMC across individual contracting offices.

CMMC training for government officials and third-party assessors should focus on ensuring consistent interpretation and application of relevant terms (including "CUI"), requirements, and security controls. To clarify applicability and consistency, DoD should update training curriculums at the Defense Acquisition University (DAU) and issue formal department-wide written instructions and guidance supplemented by FAQs or other less formal mechanisms as needed. As recently evidenced by the challenging roll-out of Section 3610 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act, the government must issue clear, consistent written guidance as early as possible to avoid widespread industry confusion or conflicting implementation among federal contracting offices. Further, DoD must pursue a continuous improvement approach to feedback, consistently seeking and incorporating feedback from industry to ensure more efficient and effective implementation. This is even more important for a complex, multi-faceted initiative like the CMMC.

Formalize Reciprocity Efforts with Other Cybersecurity Standards

While ITI fully supports CMMC's goals of increasing supply chain transparency and improving the cybersecurity posture of federal contractors, we recognize that CMMC compliance will require significant financial and resource investments by federal contractors. Many federal contractors have already made similar investments to comply with existing cybersecurity requirements. For example, Cloud Service Providers (CSPs) must achieve security authorizations under GSA's Federal Risk and Authorization Management Program (FedRAMP) or DoD's Cloud

Computing Security Requirements Guide (CC SRG). A CSP holding a FedRAMP Moderate authorization (325 NIST SP 800-53 controls) or FedRAMP High (421 NIST SP 800-53 controls) for their cloud regions and cloud services has already demonstrated compliance with the 110 baseline NIST SP 800-171 controls, as determined by a third party assessment organization (3PAO) and FedRAMP government reviewers. Additionally, authorizations like DoD CC SRG IL-4 (applies to systems handling DoD CUI) and IL-5 (applies to systems handling unclassified national security system data) have some requirements that far exceed the requirements of CMMC Level 3. Particularly when other certification requirements meet or exceed CMMC requirements, DoD should accept certifications granted by other government or established third party accreditation bodies. Where CMMC requires additional controls, or there is a difference between CMMC's organizational focus and the system level assessment of controls under other certifications, contractors should only be held accountable for demonstrating compliance with the delta of new controls, rather than the entire NIST SP 800-171 control baseline already captured under a separate certification.

For other DIB systems that are already certified to other compliance frameworks such as ISO 27002 and the American Institute of CPAs Service and Organizational Controls, we urge DoD to specifically define how these control framework certifications could be leveraged to demonstrate compliance with CMMC controls. CMMC levels must be clearly mapped to existing cybersecurity controls and frameworks, and mapping should be used consistently throughout DoD. ITI has provided a map of the relationship between CMMC levels and other cybersecurity frameworks in **Appendix I**.

To avoid duplicative compliance costs, contractors seeking CMMC certification should not be required to demonstrate security controls that are already captured in other security certification programs. This is especially important for small and medium-sized businesses where the financial burden of complying with multiple security frameworks may be a barrier to entry for government business.

Allow Prime Contractor Flexibility in Flow Down Requirements

Once fully implemented, CMMC requirements will apply to all non-COTS contracts. Accordingly, all prime and subcontractors involved in performing covered contracts will be required to achieve CMMC certification. In many cases, however, a subcontractor may not require access to CUI based on its role in the contract. This is especially true for lower-tier subcontractors such as equipment manufacturers. In addition, a subcontractor could be engaged in a working relationship where all the data stored or processed is maintained within the prime contractor's exclusive control. In these cases, it is unclear why a CMMC mandate would be imposed upon the subcontractor. We recommend that DoD provide prime contractors the sole discretion to determine when to flow down certification requirements to their subcontractors. Subcontractors should not be required to achieve and maintain CMMC certification if they have

no need to access CUI for contract performance. The government should accept the prime contractor's attestation regarding a subcontractors' CUI access.

Because the interim rule states that CMMC requirements must be included in all subcontracts or "other contractual instruments," we request clarification regarding the nature of these instruments. We urge DoD to clarify that CMMC does not apply to agreements that are not traditionally viewed as "contractual instruments," such as federal research grants, Other Transaction Authority agreements, etc. When applicable based on access to CUI, CMMC requirements should be limited to contracts and subcontracts.

Clarify Applicability to Entities Providing Commercially Available Off-the-Shelf (COTS) Products

ITI appreciates DoD's recognition that both the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) require agencies to maximize streamlined contracting procedures for commercial items—especially commercially available off-the-shelf (COTS) items. Specifically, 10 U.S.C. 2375 exempts contracts and subcontracts for the acquisition of commercial items, including COTS items, from provisions of law enacted after October 13, 1994 that, as determined by the Under Secretary of Defense for Acquisition and Sustainment, set forth policies, procedures, requirements, or restrictions for the acquisition of property or services. While we encourage DoD to comply with 10 U.S.C. 2375 by exempting *all* commercial item procurements from CMMC requirements, we strongly support the current exemption for COTS items.

To reduce confusion and ensure consistency when implementing the CMMC COTS exemption, we urge DoD to issue departmentwide guidance clarifying the definition and applicability of "COTS" for CMMC purposes. We recommend DoD's supplemental guidance provide the following clarifications:

1. A product's status as "COTS" is defined at the time of contract award. Any post-award modifications of the product to meet DoD requirements will not change the product's COTS status and will thus not trigger CMMC applicability.
2. The extent to which a prime contractor that exclusively supplies COTS products and services is exempt from all CMMC certification processes for both the products and at the organizational/enterprise level, even if the contractor will store, process, or transmit CUI. The Interim Rule notes that CMMC requirements will be phased into contracts, but contracts solely for COTS products are exempt, throwing into question whether prime contractors supplying DoD with COTS products must obtain CMMC certification[3].
3. A subcontractor that merely supplies a COTS product for use by a prime contractor is not considered to have access to CUI (regardless of whether the prime contractor must access CUI for contract performance). Accordingly, a subcontractor that supplies a COTS

[3] See 85 Fed. Reg. 61507, 61520

product for use by a prime contractor is not subject to CMMC certification requirements.

Better Define the Role CMMC Levels 4 and 5 Will Play in the DoD Cybersecurity Ecosystem

DoD should better articulate the purpose of CMMC Levels 4 and 5 and clarify in greater detail how these two levels are distinct from one another. The list of specific requirements for Levels 4 and 5 outlined in CMMC v1.02 is shorter than those for the prior maturity levels, and several domains (physical protection, personnel security, media protection, maintenance, identification and authentication) have no requirements for Levels 4 and 5 at all. Moreover, there is a disconnect between what Levels 4 and 5 require from contractors and prior statements from DoD personnel on what these levels are intended to gauge (whether the contractor engages in sophisticated practices to defend itself against APTs).

For instance, control SI.4.221, concerning system and information integrity for CMMC Level 4, states that an organization can build knowledge of Tactics, Techniques and Procedures (TTPs) by participating in Information Sharing and Analysis Centers (ISACs), and suggests that an organization "may consider" participating in multiple ISACs. However, APT information sharing can oftentimes prove to be a security threat, and the cost to safely share this information is prohibitively expensive for many companies. We suggest that DoD better outline Levels 4 and 5 in concert with industry and identify instances under which a contractor at these higher levels would be better off working with DoD to become certified in a classified environment instead of going through the C3PAO process.

Ensure an Efficient and Accountable Accreditation Body

ITI recognizes the hard work of the CMMC Accreditation Body and its volunteer members to develop standards to ensure defense industrial base cybersecurity. Given the important role of the Accreditation Body to ensure that certification process is nimble and efficient, we recommend that DoD clearly lay out the roles and responsibilities of the Accreditation Body, any additional standards-setting body that will contribute to the creation of the CMMC requirements, and any Federally-Funded Research and Development Center (FFRDC) involved in the CMMC process.

Additionally, the interim rule seems to imply that DoD and "an accreditation body" will operate as equals throughout the CMMC process. We believe the rule needs to establish safeguards to determine any accreditation organization affiliated with the CMMC is fulfilling its responsibilities in a manner that is fair to all parties involved and holds the same fiduciary duties as the government in its interaction with companies. The rule also must detail a comprehensive adjudication process between the Accreditation Body, C3PAOs, and contractors seeking CMMC certification.

We recommend that DoD provide information about how it will ensure that C3PAOs are consistent in their assessments across the DIB. How will DoD ensure that C3PAOs do not have conflicts of interest with regard to the entities they assess? The interim rule refers to a dispute adjudication process by the CMMC accreditation body related to "claimed errors, malfeasance, or ethical lapses by C3PAOs." What are the procedures for the dispute adjudication process and what are the possible outcomes? Noting that the accreditation board is not a DoD entity, will contractors be able to appeal to DoD from accreditation board decisions they dispute?

Ultimately, having a 100 percent volunteer organization serving as an accreditation body lends itself to substantial challenges. ITI suggests that DoD provide funding at least during the start-up period for the Accreditation Body to maintain staff and service members without a "pay-for-play" mentality. Since there has been substantial interest in CMMC across the federal government, utilizing the FedRAMP structure or a similar cross-department organizational effort may be ideal.

IV. Conclusion

In conclusion, we appreciate DoD's attention to our comments. ITI and its member companies stand ready to assist DoD in revising language in the development of subsequent rulemaking on this issue. We strongly support DoD's focus on optimizing cybersecurity of the defense industrial base, and we hope to collaborate further on similar matters.

Looking ahead, we believe that in order for DoD and other federal agencies to efficiently and effectively achieve security goals, there must be an effort to streamline the patchwork of requirements contractors must navigate (including the CMMC and NIST SP 800-171 as well as ITAR, CJIS, ISO 27000 series and others) into one holistic vision. A recent report released by the Cyberspace Solarium Commission, titled *Building a Trusted ICT Supply Chain*[4], includes a similar suggestion for the President to "designate a lead agency to integrate and coordinate civilian and government ICT supply chain risk management efforts into an ongoing national strategy and to serve as the nexus for public-private-partnerships on supply chain risk management." We hope to work with DoD and other government agencies to fulfill this vision and strengthen the U.S.'s commitment to a secure government and industrial base.

[4] *For more information, see* https://www.solarium.gov/public-communications/supply-chain-white-paper

Appendix I – Federal Cybersecurity Requirements for Contractors

Colored Fields Highlight Potentially Overlapping CUI Protection Requirements

Cybersecurity Scheme	Impact Level	Intended Function	Requirements
FedRAMP*	FedRAMP Low	Protect less sensitive unclassified Federal data	125 NIST SP 800-53 controls; including 29 FedRAMP controls
	FedRAMP Moderate	Protect sensitive unclassified Federal data	325 NIST SP 800-53 controls; including 66 FedRAMP controls
	FedRAMP High	Protect most sensitive unclassified Federal data	421 NIST SP 800-53 controls; including 70 FedRAMP controls
DoD Cloud Computing Security Requirements Guide*	IL-2	Protect public or non-mission critical information	FedRAMP Moderate controls
	IL-4	Protect CUI	IL-2 and CUI-specific tailored set
	IL-5	Protect higher-sensitivity CUI, mission critical information and National Security Systems (NSS)	IL-4 and NSS and CUI-specific tailored set
	IL-6	Protect classified information up to Secret level	IL-5 and classified overlay
CMMC**	Level 1	Safeguard Federal Contract Information	15 basic safeguarding requirements from FAR clause 52.204-21
	Level 2	Intermediary step for contractors as part of their progression to Level 3	65 security requirements from NIST SP 800-171, 7 CMMC practices, 2 CMMC processes

* Product Level
** Organization Level

	Level 3	Protect CUI	NIST 800-171, 20 CMMC practices, 3 CMMC processes
	Level 4	Protect CUI and reduce risk of Advanced Persistent Threats (APTs)	NIST 800-171, 46 CMMC practices, 4 CMMC processes
	Level 5	Protect CUI and reduce risk of APTs, with increased depth and sophistication	NIST 800-171, 61 CMMC practices, 5 CMMC processes

* Product Level
** Organization Level