2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

November 30, 2020

Defense Acquisition Regulations System
Attn: Ms. Heather Kitchens
OUSD(A&S) DPC/DARS, Room 3B941
3060 Defense Pentagon
Washington, DC 20301–3060

Re: Interim Rule for DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements

Ms. Kitchens:

We hereby submit our comments and outstanding questions on the Interim Rule for DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements (the "Interim Rule"). The Interim Rule will impact nearly every National Defense Industrial Association (NDIA) member.[1] Our membership comprises small-businesses and major prime contractors that form the core of our Defense Industrial Base (DIB).

NDIA fully supports the overarching policy objectives behind Section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92) and the vision of creating a unified cybersecurity standard for DoD acquisitions. NDIA has worked hard with our member companies, other trade associations, and the Department of Defense (DoD) to assist in the development of an Interim Rule to implement the Cybersecurity Maturity Model Certification (CMMC) and DoD Assessment Methodology framework. Yet, the Interim Rule has some gaps and leaves some key questions unanswered. We hope that our comments and questions will help DoD create a Final Rule.

Duplicate Assessments

In the Interim Rule, as well as in 204.7302(a)(5) and 204.7501(c), DoD indicates that NIST SP 800-171 DoD Assessments, CMMC assessments, and other DoD assessments "will not duplicate efforts where assessments are comparable, except in rare circumstances when a re-assessment may be necessary." However, DoD does not indicate which assessments and

[1]NDIA is a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)3 nonprofit organization - not a lobbying firm - and was founded to educate its constituencies on all aspects of national security. For over 100 years, NDIA has provided a platform through which leaders in government, industry, and academia can collaborate and provide solutions to advance the national security and defense needs of the nation.

levels are comparable. For example, if a contractor achieves a CMMC Level of 3 or higher, would the contractor also be required to have a NIST SP 800-171 DoD Assessment? If so, this would duplicate efforts because DoD has indicated that a CMMC Level 3 certificate demonstrates implementation of all NIST SP 800-171 security requirements. Moreover, Section VII.B "Objectives of, and Legal Basis for, the Rule" states: "This rule establishes a requirement for contractors to have a current NIST SP 800–171 DoD Assessment and the appropriate CMMC level certification prior to contract award and during contract performance." This statement, read in conjunction with DoD's statements that assessments will not duplicate efforts, further confuses the relationship between the CMMC and NIST assessment requirements. In order to avoid duplicate efforts for comparable assessments and provide clarity to contractors, subsequent rulemaking should specify which assessments and levels are comparable and allow reciprocity between comparable assessments.

Supply Chain

In the Interim Rule, "Description of an Estimate of the Number of Small Entities to Which the Rule Will Apply", states that the Basic Assessment requirement is expected to be phased in over a three-year period. This statement is the only reference to a phase-in process in this requirement, creating significant ambiguity as to how and when individual organizations might be impacted. Additionally, the rule does not detail DoD's phase-in plan for DFARS 252.204-7020(g)(2) or 252.204-7021(c)(2). Prior to this Interim Rule, subcontractors subject to implementation of NIST SP 800-171 security requirements were not required to undergo DoD assessments and it is likely that many of those subcontractors, which comprise a significant portion of the DIB, will not have completed a Basic NIST SP 800-171 DoD assessment or possess a CMMC certificate when the rule becomes effective on 30 November. Without a defined phase-in period allotting a reasonable amount of time for subcontractors to comply with these requirements contractors will find it hard to perform new contracts that use existing subcontracts and will also face limitations when entering new subcontracts. Finally, large contractors have thousands of subcontractors. A large percentage of them may handle CDI. Thus, the requirement in DFARS 252.204-7020(g)(2) for contractors to ensure subcontractors have at least a basic assessment for all covered contractor information systems relevant to the offer before making an award to a subcontractor is a significant and complex task creating significant uncertainties without a clear explanation of how this indication will reflect a bidder's cybersecurity posture. This task requires much administrative effort to ensure compliance, even assuming all subcontractors comply with the adequate security requirement of DFARS 252.204-7012. Subsequent rulemaking should 1) clarify how the

Basic Assessment requirements will be phased-in and 2) create a longer transition period (beyond 30 November)— since the 252.204-7019 provision and 252.204-7020 clause, unlike CMMC, have no limits on the number of solicitations and contracts in which they appear.

COTS and Micro-purchase Threshold

The reference to Commercial-off-the-Shelf (COTS) in the new provision and clauses does not tie directly to an official definition. Subsequent rulemaking should define COTS. Additionally, in the Preamble, DoD indicates its intent not to apply the 252.204-7019 provision or the 252.204-7020/7021 clauses to acquisitions at or below the micro-purchase threshold. To effectuate that intent, subsequent rulemaking should revise 204.7304(d) and (e), 204.7503(a) and (b), 252.204-7020(g), and 252.204-7021(c)(2), so they instruct contracting officers and contractors that the provision and clauses do not apply to acquisitions at or below the micro-purchase threshold. Additionally, in the rule we suggest citing the source that determines the micro-purchase threshold.

Controlled Unclassified Information

Our members still lack clear guidance on how to identify and mark Controlled Unclassified Information (CUI) or Covered Defense Information (CDI). It is the Government's responsibility, through the Contracting Officer, to identify CUI and CDI. Subsequent rulemaking should provide additional examples on how to identify CDI and CUI, explain the difference between the two, and outline the controls that will be in place to ensure the Services are compliant with the marking standards prescribed in DODI 5200.48. Additionally, subsequent rulemaking should identify what gaps, if any, exist between the universe of CDI and CUI covered by the rule. Guidance should also be provided to contractors, so that they understand when CUI is created as a result of their internal processes.

DFARS 252.204-7021: CMMC-Accreditation Body

DoD has partnered with a newly created third party organization, the Cybersecurity Maturity Model Certification-Accreditation Body (CMMC-AB), a Maryland-based corporation organized "exclusively as a charitable and educational organization within the meaning of section 501(c)(3) of the Internal Revenue Code of 1986."[2] The CMMC-AB will manage a cadre of CMMC Certified Assessors. The Certified Third-Party Assessment Organizations (C3PAOs) will contract with DIB companies to conduct on-site assessments

[2] CMMC-AB Articles of Incorporation, January 2020.

of DoD contractors throughout the defense supply chain. NDIA deeply appreciates the hard work of the CMMC-AB.

The CMMC-AB has adopted a Code of Ethics that appears to be aligned to the best practices of non-profit boards. Nevertheless, given that the CMMC-AB may, at times, perform inherently governmental functions, subsequent rulemaking should be in place to prevent conflicts of interest by CMMC-AB board members. Subsequent rulemaking should make clear that CMMC-AB board members:

1) Must not seek, negotiate, or accept employment which will compete with the interests of the CMMC-AB.

2) Must not accept employment or engage in any activity which will require them to disclose confidential or competition sensitive information which was gained through their CMMC-AB board service.

3) Must not disclose confidential information acquired by them during their CMMC-AB board service.

4) Must be under an ongoing obligation to disclose any actual, potential, or apparent conflicts of interest.

5) Must take appropriate steps to abate any conflict of interest, including recusal.

6) Must abstain from making personal investments in enterprises which they have reason to believe may be directly involved in CMMC-AB decisions to be made by them or which will otherwise create substantial conflicts between their duties in the public interest and their private interests.

7) Must recuse themselves in any matter in which their impartiality might be reasonably questioned or in which the CMMC-AB board member has any organizational, financial, or personal conflict of interest.

8) A CMMC-AB board member must not accept any gift or anything else having more than a nominal value under circumstances in which it could be reasonably inferred that the gift or thing of value was intended to influence the CMMC-AB

board member, or could reasonably be expected to influence the board member, in the performance of their CMMC-AB board service.

9) Must have an internal ethics advisor or advisory body to field ethics questions and conduct initial inquiries, and subsequent referral to the board if necessary, concerning ethics complaints.

Cost Allowability

Since the passage of Section 1648 of the FY 2020 NDAA, DoD has been clear that contractors need to prepare for the implementation of the CMMC Framework and DoD NIST assessments. In anticipation of the Interim Rule, many of our members have incurred costs associated with compliance. Subsequent rulemaking should provide guidance on the allowance of pre-award compliance costs and how those costs will be recovered. DoD also should consider seeking an appropriation to recover CMMC implementation costs.

CMMC Assessments & Certifications

The Interim Rule does not detail the dispute resolution process between contractors and the C3PAOs. Subsequent rulemaking should address how the government will resolve disagreements, between C3PAOs and contractors, and outline the process to appeal adverse determinations with DoD or other legal entities. Without such a process, non-DoD entities would be empowered to make procurement decisions as to whether tens of thousands of contractors would be eligible for contract awards made by the Department of Defense without any checks and balances.

CMMC and FedRAMP Reciprocity

Some of our members have expressed that the CMMC practices and NIST 800-171 requirements do not contemplate the cloud-first world that we live in, especially for small businesses. Subsequent rulemaking should allow DoD to accept GSA's Federal Risk and Authorization Management Program (FedRAMP) baselines as sufficient for CMMC compliance or expressly exempt cloud offerings from CMMC and allow FedRAMP to regulate cloud offerings. This allowance would be similar to DFARS 252.204-7012, which allows FedRAMP Moderate equivalent to meet some requirements for adequate security.

POA&Ms

Plans of Action and Milestones (POA&Ms) are not accepted under the current CMMC framework. However, other government standards allow POA&Ms as a solution to

addressing a contractor's cybersecurity issues, including the FedRAMP standard. Subsequent rulemaking should allow POA&Ms and outline the circumstances when they are permissible, and not permissible, for each CMMC level.

CMMC Level 4 and 5 Alternative

The Interim Rule includes a discussion of alternative methods of implementing CMMC Levels 4 and 5 that would require contractors to meet only a portion of the controls required by those levels, based on defined thresholds. DoD should strongly consider allowing these alternative methods. They could significantly reduce the cost to implement Level 5 by reducing the number of controls, and they will align the rest with the company's cybersecurity strategy. In addition, a variety of implementations of practices across the DIB avoids the vulnerability of a single implementation blueprint and supports defense against the Advanced Persistent Threats (APTs). Furthermore, only 18 of 41 practices at Levels 4 and 5 directly mitigate threats identified by DoD Cybersecurity Analysis and Review (DoDCAR). The other 23 practices are administrative in nature, only provide support, or enhance lower-level Practices. Overall, implementing the alternative threshold practice model (Flex Option) discussed at Levels 4 and 5 would bring critical thinking and risk management back to the CMMC model, significantly reducing cost and assessment complexity. It also would not require a change to the model or practices themselves, but rather a simpler change in assessment methodology. We recommend that DoD allow such alternatives (Flex Option) and focus on those Practices that more directly mitigate cyber threats.

Audit Standards

The Interim Rule does not give enough consideration to audit standards. DoD should consider working with the American Institute of Certified Public Accountants (AICPA) to develop audit standard for CMMC or leverage an existing audit standard that is well aligned with the CMMC framework.

Certified Third-Party Assessment Organizations (C3PAOs)

Subsequent rulemaking should require the CMMC-AB and the DoD CMMC Program Office to conduct oversight of fees charged by C3PAOs, to ensure that fees are not unreasonable. Subsequent rulemaking should also create a process to ensure consistency among the C3PAO assessments and should formalize a process for companies to resolve disputes regarding C3PAO assessments and the recourse option available to contractors and subcontractors that fail a C3PAO assessment, to include their recourse within DoD.

CMMC's Effect on New Entrants

The requirement for contractors to comply with the CMMC Framework, prior to contract award, could deter cash-strapped new entrants, and their investors, from participating in defense markets. These potential entrants may choose to enter commercial markets with lower financial barriers to entry. Subsequent rulemaking should provide some flexibility for small business new entrants to obtain CMMC certification post-contract award.

Clarity for Manufacturers

The Interim Rule does not give enough consideration to contractors that are expected to secure Operational Technology (OT) for manufacturing. Contractors that must secure OT foresee difficulties with complying with the assessments prescribed by the three clauses in the Interim Rule. For example, manufacturing systems typically cannot be frequently updated for the same reason that advanced weapon systems software cannot – significant testing is required for each software patch to ensure reliability. Outdated operating systems that cannot be patched are common. Implementing other controls, like installing anti-virus software and multi-factor authentication can also be problematic in a manufacturing environment.

Clarifying options available to manufacturers or including manufacturer specific alternatives from existing protocols, such as NIST SP 800-82 and ISA/IEC 62443, would allow manufacturers to achieve the goal of CUI cybersecurity through understood requirements.

DFARS 252.204-7019/7020 (DoD NIST Assessments Rule): CAGE Codes

The interim rule requires contractors to provide a list of CAGE Code supported by each System Security Plan (SSP). This request will often prove impractical or render results unhelpful to DoD. Large contractors have hundreds of facility CAGE Codes and many more contracting CAGE Codes. Furthermore, CAGE Codes could have a one-to-many and many-to-one relationship (e.g., one CAGE code may relate to dozens of systems, and one system may relate to many CAGE codes). For large contractors, with hundreds of facilities, use or reliance on CAGE Codes to meet a NIST SP 800-171 DoD assessment requirement for individual information systems can be confusing. Subsequent rulemaking should use a different type of unique identifier (e.g., DUNS) that would be easier to manage and better aligned with DoD's approach to the CMMC and NIST assessments.

Scope of Assessments

The requirement that the NIST SP 800-171 assessments cover "each covered contractor information system that is relevant to the offer, contract, task order, or delivery order" may lead to interpretive difficulties, particularly for contractors with multiple information systems. For larger contractors, a DIBCAC High or Medium Assessment, as well as a Basic Assessment, likely involves an assessment of a contractor's use of an "inheritance model," by which a large number of program-specific system security plans inherit protection requirements from enterprise system security plans. It is unclear how the assessment requirement would be met in such scenarios. Subsequent rulemaking should indicate how DoD will allow contractors with inheritance models to describe and score their enterprise inheritance model. Guidance would better enable contractors with such inheritance processes to meet the DoD assessment requirement by using their Medium or High DIBCAC assessments, or craft new Basic Assessments, that consider such processes. Notably, such guidance would also greatly promote the DoD's stated goals in the Preamble to 1) enable strategic assessments at the corporate-level or entity-level rather than at the program or contract level, thereby reducing cost to both DoD and industry, and 2) reduce duplicative or repetitive assessments rather than addressing implementation of NIST SP 800-71 on a contract-by-contract approach.

Source Selection

The use of a single, summary Basic Assessment score, with no additional context, may lead to a false impression of a contractor's cybersecurity posture. This is especially concerning if misleading scores were used during the source selection process. Subsequent rulemaking should provide more details on whether and how summary scores will be interpreted and acted upon by the DoD during the source selection process. Additionally, poor application of the DoD Assessment Methodology could lead to inaccurate representations in scoring. Subsequent rulemaking should provide clear liability details or a grace period to reduce industry fear of legal liability.

DFARS 252.204-7019/7020 (DoD NIST Assessments Rule): Three-year Validity Period

The Interim Rule states that the validity period for a self-assessment is three years, but the -7019 provision and -7020 clause state that the validity period is "...not more than 3 years old unless a lesser time is specified in the solicitation." The two statements are in conflict, and that introduces uncertainty. Subsequent rulemaking should include criteria as to when a lesser time might be necessary, as it will drive additional costs.

Non-U.S. Contractors

252.204-7020(c) requires contractors to provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, and 252.204-7020(g)(1) requires contractors to insert the substance of 252.204-7020 in all subcontracts and other contractual instruments excluding those solely for the acquisition of COTS items. We note the particular challenges that will accrue with non-U.S. suppliers that may have local legal and security restrictions that would restrict their ability to accept such a flow-down clause and allow U.S. representatives access to their facilities and systems. We expect that many non-U.S. suppliers will strongly push back on this requirement. Subsequent rulemaking should provide guidance on how to handle non-U.S. suppliers with conflicting legal or security obligations.

Assessment Reporting

The Interim Rule notes that contractors can send their Basic Assessments to a Navy email address via an encrypted email. However, there is no information in the Interim Rule or on the SPRS web site on how to obtain the appropriate certificate necessary to send an encrypted email. Subsequent rulemaking should provide directions on the process to obtain the appropriate certificates on the SPRS web site, or via other mechanisms, and clarify that the direct uploading of assessment scores onto SPRS is permissible for CMMC Levels 1-3. Additionally, we recommend a standalone email address for submitting assessments for entry into SPRS rather than the general SPRS support email.

Continued Proliferation of Requirements by Agencies

We are concerned that even with the onset of the new -7019 provision and -7020, and -7021 clauses, that there may continue to be a proliferation of additional, custom security requirements from various DoD agencies. Such proliferation could lead to significant inefficiencies and add to the already substantial costs that the new CMMC and DoD NIST Assessments regime will require. We recommend that DoD provide guidance to its agencies and the Services to honor the spirit of this rule, which is designed to provide the means for DoD to improve the cyber posture of contractors in a way that is cost-effective and efficient for both DoD and its contractors, rather than allowing DoD components to require disparate security requirements on a contract-by-contract basis.

Key terms are left undefined

Several terms are left undefined in the Interim Rule. Subsequent rulemakings should clearly define the words “accreditation,” “certification,” and “COTS.”

Trade Secret Protection

The Interim Rule does not provide a framework to ensure that information learned in the assessments will be subject to the trade secrets exemption under the Freedom of Information Act ("FOIA") 5 U.S.C. § 552(b)(4). Under the Interim Rule, trade secret protection is only offered as follows: "A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as 'Controlled Unclassified Information (CUI)' and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential)." The information that will be considered a trade secret under the CMMC Rule is too narrow.

Instead, all information exposed to the DoD in a medium or high assessment should be considered trade secret information. Additionally, the Interim Rule provides no assurances that a supplier may require C3PAOs to enter into a reasonable nondisclosure agreement to maintain the confidentiality of confidential information that the supplier provides to the C3PAO. The DIB would normally seek to retain as confidential most of the information released to the DoD in a medium or high assessment and to the C3PAO's in a CMMC assessment. Exposure of such information related to security measures creates a heightened security risk. The DIB and the Government's legitimate interest is to ensure the continuing confidentiality of such information. By failing to protect all information a supplier reveals in an assessment as trade secret information subject to Exemption 4 under FOIA, the Government is undermining the security of the CUI that the Government is seeking to protect by implementing the Interim Rule.

For the DoD assessment, the Interim Rule should be changed so that all information exposed in an audit, that the supplier identifies as proprietary, should be considered trade secret information, subject to Exemption 4 under FOIA. In addition, subsequent should require the C3PAO performing the assessment to enter into a reasonable nondisclosure agreement, provided that the terms of agreement do not differ from the nondisclosure agreement that a supplier typically uses with its other suppliers. The one exception to the trade secret protection should be the result of an assessment (e.g. that a contractor was certified to CMMC Level 3 on a certain date), as that information must be public to enable administration of the program.

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

Outstanding Industry Questions

On 8 October 2020, NDIA submitted a series of industry questions to Defense Pricing and Contracting (DPC). Please find an updated "Industry Questions on CMMC Implementation" letter in Appendix A. NDIA stands ready to discuss our questions in-depth. As our previous engagements on this issue show, we would be happy to participate in dialogue on the CMMC program, its requirements, and its implementation to ensure that the program achieves its objectives in a manner that meets the needs and concerns of its stakeholders.

NDIA appreciates the opportunity to comment on the Interim Rule. The point of contact for this comment is Nick Jones, NDIA's Director of Regulatory Policy, who may be reached at (703) 247-2562 or at njones@ndia.org.

Very respectfully,

National Defense Industrial Association

Appendix A

Industry Questions on CMMC Implementation

I. General Administration
   a. Is the Department incorporating into the revision of the MOU between the AB and the CMMC office guardrails around the role of the AB to ensure that it remains a ministerial functionary that will ensure equity in the accreditation of C3PAOs and the issuance of certifications and not position itself as a gatekeeper controlling access to the federal market, creating pay-to-play mechanisms to let companies be certified or other undue control over the application of the standard on the DIB companies seeking certification? If so, what are those guardrails and, if not, why not?

II. CMMC Rollout
   a. How are the pilot/pathfinder contracts being identified? Will this information be made publicly available?
   b. What information will be made public following the conclusion of the pilot/pathfinder exercises?
   c. What programs are being prioritize for CMMC rollout?
      i. Simply including this information in the RFI/RFPs may not give a company sufficient time to respond, depending on the proposal timeline, CMMC level, and especially if one is a subcontractor under the program and may not see the RFI themselves– if DoD has key aerospace competitive programs in mind they want to target in 2021, it would be helpful to share that with industry. If they plan to target certain sole-source contracts, that would also be helpful to know.
   d. Can the DoD update its FAQs online to address the most current questions about implementation from the Department's perspective?
   e. While DoD has readily made available its experts on CMMC to participate in countless industry outreach events both in person and virtually, it is not possible for members of industry to attend every event or follow every development. Will DoD commit to posting all CMMC industry events on its website as it did initially?

   f. For 2020-2025, the interim rule says it applies if the contract has both the new -7021 clause AND the SOW lists a CMMC level. What if the

RFP/contract only has the -7021 clause? DoD should give COs guidance not to include the clause (even if the rule goes into effect in 60 days) if there is no CMMC level in the SOW and it does not actually apply.

g. SPRS: How will DOD protect the basic assessment information that industry must submit into SPRS, which could be sensitive when consolidated, and what mitigations DOD will employ if SPRS is not ready by 30 November? Will SPRS have all the necessary fields needed to submit the information identified in the Interim Rule and will it use multi-factor authentication?

III. Costs

a. What additional information is currently available about the allowability of costs associate with CMMC compliance and how they will be recovered? DoD has been clear that companies need to prepare for CMMC and that has resulted in companies incurring costs associated with preparing for compliance – are they expected to be indirect costs or direct costs (for levels 4 and 5)?

b. In connection with the Regulatory Impact Analysis, has DoD included the costs that will be incurred by contractors in completing plans of action and milestones in order to achieve CMMC status?

IV. Assessments

a. Are assessments to be done on a CAGE code basis? If a contractor has multiple CAGE codes that share IT controls, will that be considered? Can a contractor schedule a single CMMC evaluation for all its CAGE codes?

V. Assessments & Certifications

a. Is the C3PAO training process prepping audit companies to understand the nuances of every different IT and manufacturing Operational Technology (OT) environment?

i. The DIB is full of technical complexity and nuance that may result in "false negatives" (failing a contractor) because the assessor lacks the technical competence and skills to understand what is likely to be many ways to approach some of the controls.

ii. How will the DoD ensure consistency of the interpretation and application of requirements between C3PAOs and government

auditors? How will the situation be handled if a C3PAO certifies a firm, but a government auditor disagrees with the findings?

b. It seems that certification audits are likely to include the target company trying to "sell" their controls to the C3PAO as adequate and sufficient to meet the standard. It is highly likely that companies will ask their outside cyber consultants to be present at the assessment to help "argue the cause." How is the CMMC-AB approaching this? Will outside cyber advisors be allowed to be present?
c. How does the DoD and the CMMC-AB plan to ensure consistency among the C3PAOs? Will there be an audit process to ensure C3PAOs are consistent and comprehensive in their assessments?
d. What oversight will there be over C3PAOs ability to set their own prices?
e. Given that the C3PAOs will be performing some traditionally governmental functions, what oversight will the DoD retain over these actors? To what extent would ethics rules applicable to Government employees be passed on to C3PAOs? For example, would any rules prevent or restrict an assessor from "switching sides" to go work for an organization seeking certification?
f. What systems and mechanisms have been developed to resolve disputes regarding C3PAO assessments, and what recourse will contractors have? Are there plans for contractors to have recourse to DoD?
g. What considerations have been given to the recourse options available to subcontractors that fail C3PAO assessments? Will this cause delay on performance of the contract? Will a subcontractor seeking to remediate shortcomings be given expedited processing for re-assessment?
h. Will C3PAOs be liable for any losses incurred due to a disputed assessment where the C3PAO was found to be in error?
i. Will DoD allow companies to use the current DCMA DIBCAC scoring methodology to count as credit during a CMMC C3PAO assessment.

VI. CMMC-AB

a. While industry recognizes the hard work of the all-volunteer CMMC-AB and their commitment to our shared mission, what legal and contractual protections are in place to prevent actual or potential conflicts of interest by Board members? Many CMMC-AB members have business interests outside the AB and the DoD itself is bound by strict ethical rules. What rules will apply to the CMMC-AB? Will these rules be included in the new Statement of Work agreement between the CMMC-AB and the DoD?

b. Will the Statement of Work between the DoD and the CMMC-AB be publicly released?
c. Has restructuring the CMMC-AB to be more in-line with the ISO model been considered?
d. Has the CMMC-AB considered a model where they hire and train assessors? This would allow the CMMC-AB more quality control mechanisms over the C3PAOs and ensure consistency in audit performance and price.
e. If the CMMC-AB does hire assessors, as the draft rule permits, how will they prevent conflicts of interest between their purported role as honest broker for the certification process and favoring their assessors in the certification process to drive business to the AB?

VII. Certification Levels

a. As many people have pointed out, there remains uncertainty about what criteria agencies will use to determine CMMC levels, how the agencies will ensure consistency in such determinations, and who will be responsible for determining CMMC levels for lower tiers. When can industry expect to see guidance on this issue to help plan for upcoming CMMC pilots?

VIII. CUI

a. Can the DoD provide an update on progress of the CUI Handbook?
b. What training and materials will be made available to contractors for the handling of CUI? Online courses? DAU materials?
c. What controls will be in place to ensure the Services are compliant with the CUI marking standards prescribed in DODI 5200.48?
d. DoD has inconsistently used the phrases "CUI" and "DoD CUI" – are they intended to be used interchangeably? Is it intended to be the same universe as today's CDI? Put differently, is there any gap between the universe of CDI today and the CUI covered by the rule?

IX. DFARS Rule

a. To what extent will there be reciprocity between the DCMA cybersecurity assessments that have been conducted to date and future cybersecurity assessments under the DFARS interim rule?
b. Will the Interim Final Rule go into effect immediately upon issuance, thereby enabling the Services to invoke the CMMC in new contracts, Mods, SOW

change orders; or will it be restricted to only new contracts in accordance with the CMMC phased roll-out?

c. The Interim Rule says COs have to verify, "for contractors that are required to implement 800-171", that contractors have an active assessment before they can award contract extensions – will the requirement to have an assessment will apply to existing contracts who have an option exercised after the effective date?
d. The Interim Rule says COs must verify, "for contractors that are required to implement 800-171", that the contractor has a current assessment. Does that mean only contractors who receive CUI (and trigger the clause) must submit? Or any contract that contains the -7012 clause will be required to submit? Many contracts may contain the -7012 clause, but no CUI is exchanged or generated, and it would be helpful to provide guidance to contracting officers about this distinction.
e. How will DoD decide when to do a medium or high assessment?