CMMC and the Three "Cs": Cost, Conflicts and Competition

June 3, 2020

A. Introduction and Key Take-Aways

The Department of Defense's (DOD) Cybersecurity Maturity Model Certification (CMMC) program provides a metric for independent third parties to use in assessing and certifying the progress of the approximately 300,000-350,000 contractors and subcontractors in DOD's supply chain towards adequate cyber safeguarding of confidential information, including controlled unclassified information (CUI), located on their information systems. The CMMC program is intended to supplement, and not supersede, the existing cybersecurity requirements of the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS), including DFARS clause 252.204-7012, which incorporates the information security standards and controls of NIST SP 800-171. Implementation of CMMC will affect DOD contractors and subcontractors in many ways, but its greatest impacts will be on cost, conflicts and competition. This article examines the impact that CMMC will have on each of these areas. In particular:

- Cost. DOD officials have stated publicly that CMMC costs are allowable, but that statement is too broad for contractors to rely on. To begin with, there is a wide range of costs that could be considered "CMMC costs," from the fees the contractor pays a third party to assess the maturity level of its information systems to the labor, software, professional and IT investment costs necessary to raise the maturity level of those systems to the desired CMMC level. The allowability of these costs depends on a number of factors, including the nature and amount of the costs, the manner in which the contractor has accounted for them and similar costs in the past, and the method for allocating such costs to government contracts. Furthermore, even if a particular contractor's CMMC costs are deemed allowable, the contractor may not be able fully to recover those costs due to competitive pressures and other factors.
- Conflicts. Implementing CMMC will create potential conflicts of interest for most if not all participants in the program. Such participants include the third parties who will assess contractor's CMMC maturity levels, the members of the board of directors of the non-profit organization charged with training and accrediting those assessors, and the contractors and subcontractors seeking CMMC certification.

Contact Information

If you have any questions concerning this alert, please contact:

Bob Huffman
Partner
rhuffman@akingump.com
Washington
+1 202.887.4530

Scott Heimberg
Partner
sheimberg@akingump.com
Washington
+1 202.887.4085

Angela Styles
Partner
astyles@akingump.com
Washington
+1 202.887.4050

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington
+1 202.887.4308

Some of these potential conflicts of interest could be considered organizational conflicts of interest (OCIs) that, if not properly avoided, mitigated or waived, could form the basis for bid protests.

- Competition. DOD intends to make certification at a specified CMMC maturity level a "go/no go" evaluation factor in future procurements. This will likely limit the ability of some firms, particularly small businesses, to compete for DOD contracts and subcontracts. DOD's authority to condition eligibility for award on certification at a particular CMMC maturity level is likely to be upheld as a reasonable restriction on competition in light of the national security imperative to enhance supply chain cybersecurity. However, the manner in which DOD applies the CMMC certification requirement in a particular procurement, as for example in determining which proposed subcontractors must be certified to which CMMC levels, is likely to be challenged in particular procurements as unduly restrictive of competition or otherwise unreasonable. In addition, it is unclear what role CMMC certifications will play in determinations of the responsibility or non-responsibility of particular offerors.

B. Background

1. The DFARS Cyber Rule

The DFARS has, since 2013, imposed mandatory information security and cyber incident reporting requirements on DOD contractors and subcontractors. These requirements are currently found in DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec. 2019) (DFARS–7012),[1] and related DFARS clauses and provisions. DFARS–7012 is mandatory for all DOD prime contracts except contracts for commercial-off-the-shelf (COTS) items.[2]

DFARS–7012 requires the contractor to provide “adequate security” for all “covered contractor information systems.”[3] Adequate security is defined to mean “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.”[4] Adequate security requires at a minimum that the contractor implement the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”[5] The contractor “shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.”[6]

DFARS–7012 requires application of the NIST 800-171 standards to a “covered contractor information system,” which is defined to mean “an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.”[7] Covered defense information (CDI) is defined as “unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/CUI/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government policies, *and* is —

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; *or*

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."[8]

In addition to imposing data safeguarding requirements, DFARS–7012 requires the contractor to report all "cyber incidents" to DOD that affect a covered contractor information system or the CDI resident thereon.[9] The clause defines "cyber incident" as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."[10] The term "compromise" means "disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred."[11] Contractors who discover a cyber incident affecting CDI (or an information system housing CDI) must: (1) conduct a review for evidence of compromise of CDI, (2) report the cyber incident within 72 hours of discovery to DOD at https://dibnet.dod.mil, (3) preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days, (4) isolate malicious software and submit such software to the DOD Cyber Crime Center ("DC3") in accordance with instructions provided by DC3 or the cognizant contracting officer and (5) provide DOD with access to additional information or equipment necessary to conduct a forensic analysis and damage assessment.[12]

Contractors must include the DFARS–7012 clause verbatim (except for the identity of the parties) in all subcontracts "or similar contractual instruments" for operationally critical support or for which subcontract performance will involve CDI.[13] Contractors must also require subcontractors who report cyber incidents to DOD to provide the prime contractor (or next higher-tier subcontractor) with the incident report number assigned by DOD as soon as practicable.[14]

By offering a proposal to DOD for a contract that will include DFARS-7012, the offeror represents that it "will implement the security requirements specified by [NIST 800-171] . . . not later than December 31, 2017." As a result, as of January 1, 2018, each such proposal to DOD amounts to a representation that the contractor has implemented the NIST SP 800-171 security requirements. In making this representation, a large number of offerors have relied on informal guidance from DOD that implementation of the NIST SP 800-171 security requirements (and therefore compliance with DFARS-7012) can be demonstrated by completion of a System Security Plan ("SSP)" and/or a Plan of Actions and Milestones ("POAM") that identifies any unmet NIST SP 800-171 requirements and includes plans and milestones for achieving full compliance with those requirements. DOD's informal guidance has been that such SSPs and POAMs are sufficient to demonstrate compliance with DFARS-7012, even if full compliance with all NIST SP 800-171 requirements occurs after December 31, 2017.[15]

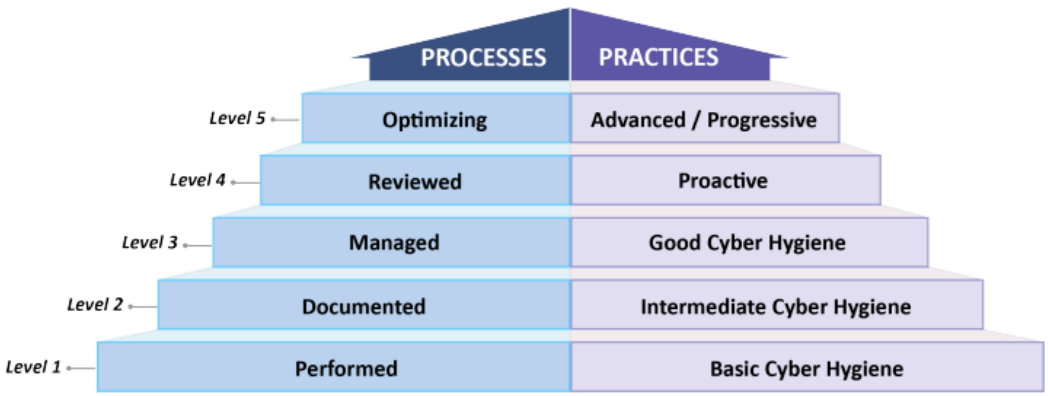
2. The Emergence of CMMC

Notwithstanding the data safeguarding requirements of DFARS-7012, DOD's supply chain experienced a number of sophisticated cyberattacks during 2018 and 2019 that revealed significant deficiencies in the cybersecurity capabilities and maturity of many of the contractors and subcontractors in the supply chain, particularly at the lower levels. The most significant of these attacks was on a lower-tier Navy

supplier that resulted in the exfiltration, presumably by a foreign adversary, of technical specifications for an advanced Navy antisubmarine warfare system.[16] This and other attacks prompted U.S. Government Accountability Office (GAO),[17] the DOD OIG[18] and many in Congress[19] to question the adequacy of DOD's cybersecurity efforts. In particular, many questioned whether contractor self-attestation of compliance with DFARS–7012 and NIST 800-171 standards provided a sufficient basis for protecting CDI at all tiers of DOD's supply chain.

In response to these concerns and the continued threat of loss of critical technical information in the hands of its suppliers, the Assistant Secretary of the Navy for Acquisition, James Guerts, issued a memorandum in September 2018 (the "Guerts Memorandum") directing Navy program managers and contracting officers to include "enhanced" cybersecurity protections in new Navy contracts for critical systems or components or involving critical technology that went beyond the requirements of DFARS–7012 and even NIST SP 800-171.[20] Other DOD components, including the Missile Defense Agency, also began insisting on cybersecurity requirements that went beyond the requirements of DFARS–7012 and NIST SP 800-171.[21]

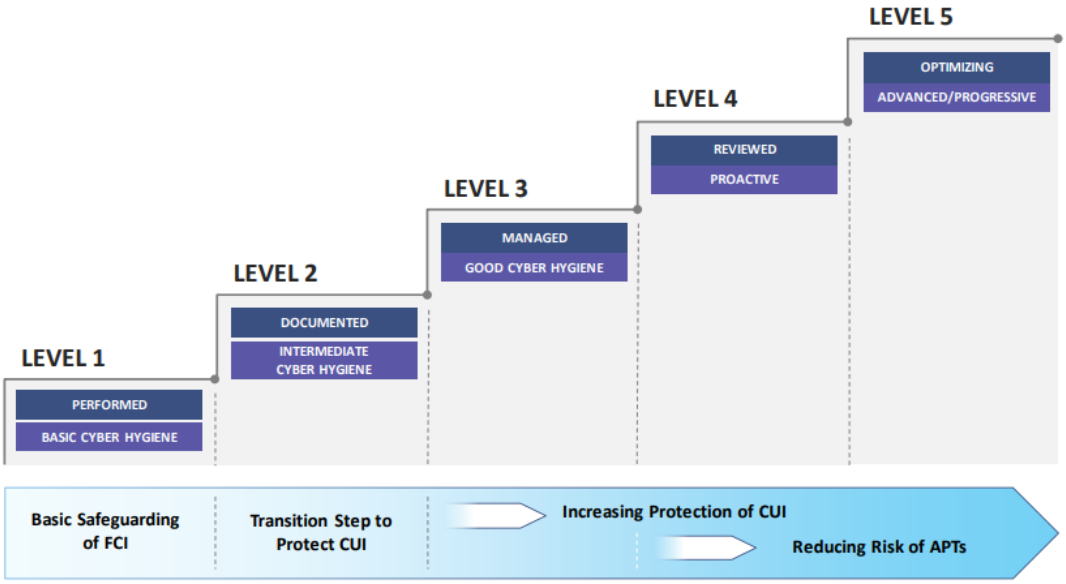
Faced with widespread criticism of DFARS–7012's self-attestation feature, and the prospect that multiple DOD components would impose varying and potentially inconsistent cybersecurity requirements, the Office of the Under Secretary of Defense for Acquisition and Sustainment, in partnership with Johns Hopkins University, Carnegie Mellon University, the Defense Industrial Base Sector Coordinating Council and various aerospace and defense trade associations, developed the CMMC program.[22] CMMC is a metric for independent third parties to use to assess and validate the cybersecurity practices, processes and relative maturity of the information systems of the approximately 300,000–350,000 firms that DOD estimates are in its supply chain.[23] CMMC Version 1.02, which DOD released on March 18, 2020, incorporates cybersecurity standards from various sources, including NIST SP 800-171, and will (when fully implemented) result in assignment of one of five CMMC maturity levels to the information system(s) of each of these 300,000-350,000 firms based on the processes and practices shown below:[24]



CMMC Levels 1-5 are cumulative.[25] This means that, in order for a company to be certified at a particular CMMC level, say Level 5, it must demonstrate achievement of the preceding lower levels, in this case Levels 1-4.[26] Furthermore, the company must demonstrate both the requisite institutionalization of processes (the left side of the above figure) and the implementation of practices (the right side of the figure) in order to qualify for certification at a particular CMMC level.[27] In those cases where the

company demonstrates different levels of process and practice implementation, the company will be certified at the lower of the two.[28] Thus, in the case of a company whose process institutionalization is found to be at CMMC Level 5 and practice implementation is found to be at CMMC Level 4, the company would be certified at CMMC Level 4.[29]

The five CMMC levels shown above provide a means of aligning a company's maturity processes and cybersecurity practices with the type and sensitivity of the information to be protected and the range of threats to be protected against. Thus, for example, CMMC Level 1, Basic Cyber Hygiene, is adequate for a system that houses or transmits Federal Contract Information (FCI) and consists of the practices that correspond to the basic safeguarding requirements specified in the FAR Basic Cybersecurity Clause, FAR 52.204-21.[30] CMMC Level 3, Good Cyber Hygiene, is designed for systems that house or transmit Controlled Unclassified Information, which includes CDI, and its standards correspond to the NIST 800-171 standards incorporated into DFARS-7012 (plus 20 additional non-NIST standards).[31] The top two CMMC Levels, Levels 4 and 5, are designed to protect CUI and critical systems or technologies against Advanced Persistent Threats (APTs) and consist of the draft standards of NIST 800-172 for APTs as well as certain non-NIST standards.[32] The chart below illustrates the correlation of the CMMC maturity levels with the type of information and threat involved:[33]



DOD intends to use the five CMMC maturity levels as "go/no go" evaluation criterion in future procurements.[34] The requests for information (RFIs) and requests for proposals (RFPs) for these procurements will identify a particular CMMC level for the prime contractor, and the same or different CMMC levels for some or all of the subcontractors, as a requirement for award of the contract.[35] Offerors (and presumably their subcontractors) will be required to be certified at the CMMC level identified in the RFP by the time of award.[36] Offerors who could not demonstrate the ability or likelihood of being certified at the required CMMC level would not be eligible for award and could presumably be excluded from the competitive range. The requirement to be certified at a particular CMMC level in order to be eligible to compete for and win valuable government contracts provides a powerful incentive for the DOD industrial

base to improve and harden their cybersecurity defenses as necessary to achieve and maintain certification at the required CMMC level.

3. CMMC Implementation

Third party assessment of CMMC maturity levels will be performed by accredited (licensed) assessors employed by accredited (certified) CMMC Third Party Assessment Organizations (C3PAOs), all of which will be accredited and overseen by a private non-profit corporation known as the CMMC Accreditation Board (AB).[37] The responsibilities of the AB are delineated in a Memorandum of Understanding (MOU) between DOD and the AB that was executed on March 23, 2020. The AB's responsibilities include (1) developing a standard that accredited assessors will use to determine the threshold of evidence necessary to validate each control in the CMMC; (2) training and accrediting potential assessors and C3PAOs and (3) certifying contractors' CMMC levels based on the assessments by the C3PAOs and individual assessors. The AB may also resolve disputes between C3PAOs and contractors regarding the merits of particular C3PAO assessments, and possibly between contractors and the AB itself regarding the merits of particular AB certifications.

The AB maintains a website detailing its plans and progress for carrying out its responsibilities under its MOU with DOD. AB anticipates that it will begin training a limited number of candidate assessors in late June or early July 2020, and begin identifying and registering entities seeking to be accredited as C3PAOs in roughly the same period. It remains to be seen whether the coronavirus pandemic and resulting shut-downs will impact this schedule.

DOD originally intended that a CMMC level requirement would appear in all RFIs beginning in June 2020 and all RFPs beginning in September 2020. However, faced with considerable push back from industry and the lack of trained and accredited third-party assessors, DOD decided to implement CMMC on a rolling basis beginning with 10 to 15 "pathfinder contracts" in the Fall of 2020 (FY 2021) and extending to an increasing number of additional contracts over the next five fiscal years. An example of this implementation plan is set forth in the following table:[38]

Total Number of Contracts with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	895	4,490	14,981	28,714	28,709
Level 2	149	748	2,497	4,786	4,785
Level 3	448	2,245	7,490	14,357	14,355
Level 4	4	8	16	24	28
Level 5	4	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

As can be seen from the above table, required CMMC levels would appear in the RFPs for approximately 1,300 DOD contracts during FY2021–2025, affecting approximately 130,000 DOD prime contractors and subcontractors (100 contractors per contract). This leaves approximately 170,000–220,000 contractors in DOD's 300,000–350,000 member supply base unaffected by CMMC requirements until at least FY2026. Although the table above states "all new DOD contracts will contain the CMMC requirement in FY26," the number of such contracts would be insufficient to bring all of the remaining firms in the supply base under CMMC requirements in that year. DOD officials have informally suggested that it could be 2030 or 2031 before all of the 300,000–350,000 companies estimated to be in DOD's supply chain are subject to CMMC assessment and certification.

In addition to rolling out CMMC over several years, DOD also made several changes that will make it easier for its supply base to adapt to the program. First, DOD reversed its previous position that CMMC would apply to COTS contractors and subcontractors and agreed that firms that sell only COTS items will NOT be subject to CMMC.[39] (However, CMMC will apply to all other agreements involving DOD funding, including grants, cooperative agreements and other transaction agreements (OTAs), as well as foreign contractors and subcontractors.) Second, DOD has stated that the CMMC assessment and certification process would give contractors credit for preexisting cybersecurity certifications, including ISO certifications, FedRAMP certificates, authorizations under DOD's Cloud Computing Security Requirements Guide (SRG) and DCMA assessments.[40] Finally, after initially expressing the position that each firm would be assessed an enterprise CMMC level (i.e., one CMMC level for the entire company), DOD acknowledged that it would be more realistic and efficient to assess CMMC maturity levels at the "enclave" (e.g., segments, systems, legal entities) level.[41] This could result in several, indeed many, CMMC certified levels for a particular company.

Finally, DOD has announced its intent to propose a DFARS regulation that will address the implementation of CMMC in DOD contracts.[42] This proposed regulation will likely include one or more DFARS clauses for inclusion in solicitations and/or contracts that would, among other things, require the contractor to maintain the CMMC maturity level required by the solicitation, undergo reassessment and recertification of its CMMC maturity every three years and presumably flow down to its subcontractors the CMMC maturity level requirement for such subcontractors that appears in the solicitation. DOD has expressed the hope that this DFARS regulation will have become final by October or November 2020 when DOD expects the RFPs for the "pathfinder" contracts with CMMC requirements to be issued, however this timeline may be delayed due to COVID-19-related restrictions, including the difficulty of holding a public meeting on the proposed regulation during the pandemic.[43] As of May 28, 2020, DOD's proposed rule implementing CMMC requirements is pending with the Office of Management and Budget's Office of Information and Regulatory Affairs.[44]

C. CMMC and the Three "Cs": Cost, Conflicts and Competition

CMMC will affect DOD and its supply chain in many ways. Three of its most significant impacts will be on cost, conflicts and competition. This section looks at CMMC's impact in each of these areas.

1. Cost

Ms. Katie Arrington, the Chief Information Security Officer of the Office of Undersecretary of Defense for Acquisition and Sustainment, and DOD's principal spokesperson for the CMMC program, has stated publically that CMMC costs are "allowable."[45] She has also stated that the DOD wants contractors to build the cost of CMMC into their rates.[46] These statements appear to be intended to allay contractor concerns, particularly among small and medium size businesses, that obtaining CMMC certifications will be unduly expensive or otherwise adversely affect their ability to compete for DOD work. However, Ms. Arrington's assertion that CMMC certification costs are allowable does not guarantee that any particular contractor's or subcontractor's cost of CMMC certification or of achieving a particular CMMC maturity level will be determined to be allowable or that the contractor or subcontractor will be able to recover those costs in the prices of its DOD contracts. Rather, the allowability of a contractor's or subcontractor's CMMC costs, and its ability to recover those costs, will depend on several factors, including the type of costs in question, the reasonableness of those costs in nature and amount, whether and how the contractor accounts for and allocates similar types of costs, and the type of contract under which the costs are sought to be recovered.

a. Allowability

FAR 31.201-2 states that a cost is allowable if it complies with **all** of the following requirements:[47]

(1) Reasonableness.

(2) Allocability.

(3) Standards promulgated by the Cost Accounting Standards (CAS) Board, if applicable, and generally accepted accounting principles and practices appropriate to the circumstances.

(4) Terms of the contract.

(5) Any limitations set forth in subpart 31.2.

Given the lack of any express limitation on CMMC costs in FAR Subpart 31.2, the allowability of any particular CMMC cost will likely depend upon the first four factors identified above, namely (a) the reasonableness of the cost; (b) the allocability of the cost; (c) how the cost is accounted for under CAS, GAAP, and other appropriate accounting practices and (d) the terms of the particular contract or contracts under which the cost is sought to be recovered.

i. Reasonableness

FAR 31.201-3 states that a cost is reasonable "if in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of competitive business."[48] What is reasonable depends upon a variety of considerations and circumstances, including whether "it is a type of cost generally recognized as ordinary and necessary for the conduct of the contractor's business or the contract performance."[49] The fees paid by a contractor to a C3PAO for a third-party assessment and certification of its information system(s), as well as the costs incurred

by the contractor during that process, would appear to be reasonable in nature given the requirement to have CMMC certification(s) in order to compete for certain government contracts and subcontracts. That requirement makes the costs of obtaining such certifications necessary for the performance of such contracts and for the conduct of the contractor's business. Furthermore, fees paid to the C3PAO, as well as the costs incurred by the contractor during the C3PAO's assessment and certification process, would appear to be reasonable in amount if they are roughly equal to the fees paid and costs incurred by similarly-situated contractors. It is worth noting in this regard that the AB does not intend to set the fees that C3PAOs can charge contractors for providing CMMC assessments and certifications, so contractors will have to rely on competition among C3PAOs to keep those fees in check.

Of course, CMMC costs will include more than just the fees paid the C3PAO. They will also include the costs of preparing for the C3PAO assessment and certification process, including in some cases the costs of upgrading the security of the contractor's or subcontractor's information systems to the desired CMMC maturity level(s). While the costs of achieving CMMC Level 1 may not be significant for most government contractors or subcontractors given the fact that the FAR already requires contractors handling federal contract information ("FCI") to meet the NIST SP 800-171 standards that are incorporated in CMMC Level 1, the costs of achieving CMMC Levels 4 or 5 would be considerable for most contractors and subcontractors except perhaps the 10 or so largest DOD prime contractors. Indeed, even achieving CMMC Level 3 will be costly for some contractors and subcontractors (particularly small businesses) given their current dependence on SSPs and POAMs to demonstrate their implementation of the NIST SP 800-171 under DFARS-7012.

Whether it would be reasonable for a contractor or subcontractor to incur substantial costs to increase the maturity of a particular information system to the level required by CMMC Levels 3, 4 or 5 will depend on the opportunities that the contractor or subcontractor is likely to have to compete for contracts assigned those levels, the amount of revenue that the contractor or subcontractor reasonably anticipates receiving from such contracts, and the costs the contractor or subcontractor would be required to incur to achieve those levels. For example, it may not be reasonable for a contractor to spend millions of dollars to achieve a CMMC maturity level of CMMC Level 5 if it is likely to have the opportunity to compete for only a relatively small number of CMMC Level 5 contracts. Of course, it is difficult to predict how many such contracts there will be. Furthermore, the contractor could always seek to justify the reasonableness of costs incurred to achieve CMMC Level 4 or 5 maturity on the grounds that such maturity is necessary to enable the contractor to ensure the protection of its and its customers' information from APTs.

Assessing the reasonableness of costs incurred to achieve CMMC Level 3 maturity presents additional issues because contractors who handle CDI are already required by DFARS-7012 to meet the security requirements of NIST SP 800-171. In this regard, DOD Assistant Secretary for Acquisition Kevin Fahey has stated publicly that DOD should not have to pay contractors for meeting their existing contractual requirements.[50] However, a contractor could still show that its costs of obtaining a Level 3 certification were reasonable if (1) such costs were necessary to meet the 20 or so requirements of Level 3 that go beyond the requirements of NIST SP 800-171, or

(2) the contractor had an SSP and POAM that showed that the contractor has not yet fully implemented all of the NIST SP 800-171 requirements.

The planned implementation of CMMC on an "enclave" basis rather than an "enterprise" basis raises the possibility that a contractor or subcontractor will incur costs associated with obtaining multiple certifications. Indeed, one CMMC AB Board member stated publically that a large prime contractor may require "thousands" of CMMC certifications.[51] The reasonableness of preparing to obtain and obtaining numerous CMMC certifications will depend upon the contractor's particular business organization, information system architecture and IT capabilities. It is difficult to imagine that contractors and subcontractors will spend money to create or certify enclaves that do not need to be created or certified for legitimate business reasons. Accordingly, so long as the Defense Contract Audit Agency and the contracting officer responsible for auditing and authorizing contract costs understand the purpose and legitimacy of multiple CMMC certifications per contractor, the reasonableness of the cost of such certifications should not be too difficult for the contractor to demonstrate.

ii. Allocability

In order for a particular cost to be allocable, it must be "assignable or chargeable to one or more cost objectives on the basis of relative benefits received or other equitable relationship."[52] Subject to this principle, a cost is allocable to a government contract (or other final cost) if it:

(a) Is incurred specifically for the contract.

(b) Benefits both the contract and other work and can be distributed to them in reasonable proportion to the benefits received. or

(c) Is necessary to the overall operation of the business, although a direct relationship to any particular cost objective cannot be shown.[53]

Most CMMC costs would appear to be allocable to contracts or other final cost objectives under one of the three scenarios described above. To the extent that there is only one RFP that requires CMMC certification on the part of a particular contractor or subcontractor, that contractor or subcontractor could reasonably argue that the costs of preparing for and supporting a C3PAO audit and certification is incurred specifically for that contract and therefore is allocable as a direct cost of that contract. This argument becomes more difficult when applied to capital, labor, professional, and other costs incurred by the contractor to achieve a particular CMMC level. Those costs would appear to benefit both the contract with a specified CMMC requirement and other work or be necessary to the overall operation of the business, and therefore allocable as indirect costs. Under such circumstances, such costs would properly be regarded as part of overhead or general and administrative (G&A) costs and recoverable through the overhead or G&A rates that the contractor uses in proposals and billings for government contracts. Consistent with this view, Ms. Arrington has stated more than once that CMMC costs would be part of contractor rates.[54]

iii. Consistency with FAR, CAS and appropriate accounting practices.

In addition to being allocable to contracts (or other final cost objectives) under the principles discussed above, the contractor's treatment of CMMC costs as direct or indirect costs, and the methods used by the contractor to allocate these costs to contracts, must be consistent with the FAR, CAS (if applicable) and other accounting practices, including the contractor's established practices for accounting for similar costs. FAR 31.202 imposes requirements for direct costs, including the requirement that no cost objective shall have allocated to it as a direct cost any cost "if other costs incurred for the same purpose in like circumstances have been included in any indirect cost pool to be allocated to that or any other final cost objective."[55] Likewise, FAR 31.203 and CAS 401 and 402 require consistency in the treatment of indirect costs, including the requirement that the contractor accumulate indirect cost by logical cost groupings with due consideration for the reasons for incurring such costs, and that the contractor use an allocation base for each such grouping that is common to all cost objectives to which the grouping is to be allocated.[56] In addition, for those contractors or subcontractors that are required to submit CAS Disclosure Statements, the contractor's treatment of CMMC costs should be consistent with the contractor's disclosed accounting practices unless the government approved (or CAS required) a change in the contractor's cost accounting method.[57]

Each of these accounting practice requirements potentially affects a contractor's treatment of its CMMC costs. For example, if a contractor has historically accounted for the costs of its IT organization or software as an overhead or G&A cost, or recovered such costs through overhead or G&A rates, it could not begin treating such costs as direct costs of a particular DOD contract simply because the RFP for that contract identified a required CMMC level in order to be eligible to bid for the contract. Instead, the contractor would appear to be required at a minimum to disclose its change in accounting practice and obtain the government's approval thereof, perhaps in the form of an Advance Agreement pursuant to FAR 31.109.[58] Likewise, the contractor would likely have to obtain the government's permission, or at least disclose to the government, any decision to begin grouping particular costs or investments as "CMMC costs" that it had previously grouped in other cost categories.

iv. Consistency with the terms of the contract.

In addition to the allowability factors discussed above, the charging of a particular cost to a contract must be consistent with the terms of that contract. Thus, for example, if the allowable cost clause of a particular contract contains special provisions for or limitations on the allowability of a particular cost, that clause could limit the allowability of a cost that is otherwise allowable. This could affect CMMC costs in several ways. For example, if the CMMC costs were incurred prior to award of a contract (i.e., in order to obtain the certification necessary for award of the contract), their allowability could be positively or adversely affected by the presence of a contract clause dealing with pre-award costs. Alternatively, the contract could include a clause specifically dealing with the allowability (and recovery) of CMMC costs, or particular categories of such costs, under the contract. Indeed, it is possible that the anticipated proposed DFARS rule regarding implementation of CMMC in contracts will address, or include DFARS clauses addressing, the allowability or recovery of CMMC contracts.

The inclusion of any such DFARS clauses in a specific contract could make particular CMMC costs allowable or unallowable.

b. Recoverability of Allowable CMMC Costs

Just because a cost may be allowable does not mean that a contractor will be able to recover it. For example, while a DOD contractor or subcontractor competing for a firm fixed-price contract or subcontract may be free to increase its proposed price to recover some or all of its CMMC costs (however determined), it runs the risk that increasing its proposed price could make that price uncompetitive. Thus, competitive forces may compel the contractor or subcontractor to absorb some or all of its CMMC costs in order to better its chances of winning.

Indeed, recovery of allowable CMMC costs is not guaranteed even in the case of cost reimbursement type contracts or flexibly priced contracts. For example, to the extent that a contractor includes all of its costs of obtaining a CMMC certification in its cost proposal for a particular cost reimbursement or flexibly priced contract (i.e., the first contract for which it bids that requires that CMMC level), the contractor risks increasing its proposed cost above that of its competitors or the government's cost estimate. Even a sole source cost proposal could be rejected by DOD if it concluded that inclusion of the CMMC costs made the cost too high or shifted a disproportionate amount of the CMMC costs to the particular contract. Furthermore, in the case of a cost reimbursement type contract or fixed price contract that exceeds the Truthful Cost and Pricing Act threshold (currently $2 million) and is not otherwise exempt, the contractor would be required to certify that it had submitted current, accurate, and complete cost or pricing data, including CMMC cost data.[59] Furthermore, even where an exemption from certified cost or pricing data applied, the contractor could be required under certain circumstances to provide other than certified cost or pricing data, which again could include CMMC cost data.[60] Both of these requirements would require contractors to carefully track and document their CMMC costs.

2. Conflicts

Several features of CMMC could give rise to potential conflicts of interest. To begin with, the members of the AB's Board of Directors, all of whom have other jobs, will exercise considerable influence over the AB's interpretations of the CMMC standards, its decisions regarding the accreditation and training of C3PAOs and the certification of firms in the supply chain. Unless restrained by rules and guidelines, AB Board members could use their influence to advance their own personal interests or the interests of their employer or existing or potential clients. Second, C3PAOs and their individual assessors face actual or potential conflicts to the extent they assess companies for whom they perform other services, or have performed services in the past. C3PAOs may also create conflicts or the appearance of conflicts to the extent that they or other parts of their organization seek CMMC certification for themselves in order to compete for government contracts or subcontracts that have CMMC requirements. Finally, relationships between DOD, the AB, C3PAOs and DOD contractors and subcontractors could create actual or potential "OCIs" that, unless avoided, mitigated, or waived, could result in successful bid protests by disappointed bidders in procurements with CMMC requirements.

a. Potential AB Conflicts

The AB is a private, not-for-profit corporation organized under the laws of the State of Maryland. It has a board composed of 15 directors, all of whom are professionals employed by other organizations, including DOD contractors and their vendors. These directors are responsible for developing and approving the assessment guidance and training that the AB will provide to candidate C3PAOs. Also, because the AB currently has no professional staff, some or all of the AB directors will participate in, and ultimately be responsible for, deciding which candidates become accredited assessors and C3PAOs and which contractors are certified at which CMMC levels.

The significant role played by the directors in the AB's guidance, training, accreditation and certification functions create significant potential for conflicts of interest. For example, a director who is employed by a likely C3PAO candidate or consultant to such a candidate could use his or her authority over the guidance or accreditation process to make it easier for that candidate to be accredited. That director could also influence the AB's decision to certify (or not to certify) a particular contractor at a particular CMMC level.

In recognition of these potential conflicts, the AB Board has adopted a code of ethics for its Board members. This code imposes the following duties on each AB Board member: (1) a Duty of Care; (2) a Duty of Loyalty and (3) a Duty of Compliance.[61] The Duty of Care obligates the Board member to "ensure that the organization makes prudent use of all things within the leadership's care," including "how the organization respects and nurtures its people, preserves and protects the resources being managed, and maintains the public trust placed upon the organization and its leadership."[62] The Duty of Loyalty provides that the member must "take[] actions that are in the best interest of the mission, placing service before self, avoiding/addressing conflicts of interest consistent with the CMMC-AB Conflict of Interest Policy, safeguarding confidential information and refraining from the pursuit of private gain."[63] Finally, the Duty of Compliance provides that the member "must, now and always, obey all applicable laws, regulations, commitments, governance documents, and best practices in both actions and appearances."[64]

The CMMC-AB Conflicts of Interest Policy referenced in the Duty of Loyalty above has not yet been issued. When issued, it may address with greater specificity the types of situations that could create conflicts for members of the AB Board of Directors.

b. Potential Assessor Conflicts

C3PAOs and their individual accredited assessors could encounter significant conflicts of interest once they are accredited and begin competing with other C3PAOs for assessment work. For example, a firm seeking certification may feel more comfortable if the C3PAO assessors who are performing the CMMC level assessment are part of the firm's regular outside accounting firm or other consulting or professional services firms. Ms. Arrington and other DOD spokespersons have stated that professional services vendors who are currently doing work for a company would lack the independence to perform third-party CMMC assessment and certification activities for that company.[65] These representatives have similarly asserted that a C3PAO organization whose employees perform CMMC assessments and certifications for a

particular company should not be permitted to sell information security products, solutions or software to that company.[66] At this stage, it is unclear who would enforce these prohibitions and over what period they would be enforced.

c. Potential Contractor Conflicts

CMMC certification creates the potential for conflicts of interest between contractors competing for DOD contracts that have CMMC level requirements. These conflicts could take the form of "OCIs", although they could take other forms as well.

The relevant GAO and Court of Federal Claims case law identifies three general categories of OCIs: (1) where the contractor has conflicting roles that could impair its ability to provide independent and objective advice or services to the government ("impaired objectivity OCI"); (2) where the contractor could use its contractual position to influence the rules or requirements of a contract solicitation in a manner that favors it or associated companies in competing for that or a subsequent contract ("biased ground rule OCI"); and (3) where the contractor's performance of a government contract or subcontract gives it access to non-public information that results in an unfair competitive advantage over other offerors ("unequal access to non-public information OCI").

Of these three categories, solicitations involving CMMC requirements would appear to be particularly susceptible to biased ground rule OCIs and unequal access to information OCIs. For example, to the extent that a particular offeror or its affiliate participated with government program managers or others in determining the CMMC level that offerors for a particular prime contract or subcontractor would be required to meet, such participation could be viewed as creating an actual or potential biased ground rules OCI. An example of an actual or potential unequal access to nonpublic information OCI would be if one of the offerors for a contract with a CMMC requirement, through its performance of a government contract, gained access to non-public and competitively useful information related to the cybersecurity performance or capabilities of a competing offeror or its proposed subcontractors.

Regardless of the type of OCI potentially involved, the identification of a potential OCI in a particular procurement "is a fact-specific inquiry that requires the exercise of considerable discretion." *Guident Techs., Inc*., B-405112.3, 2012 CPD 166. (June 4, 2012). FAR 9.505 requires contracting officers to use common sense and exercise good judgment and sound discretion to (1) determine whether a significant potential OCI exists and (2) to determine an appropriate means for resolving it.[67] GAO and the courts review a contracting officer's OCI investigation and determination for reasonableness, and "where an agency has given meaningful consideration to whether a significant conflict of interest exists, we will not substitute our judgment for the agency's absent clear evidence that the agency's conclusion is unreasonable."[68] Furthermore, even where a protestor provides "hard facts" demonstrating the potential existence of an OCI, and the agency fails to meaningfully consider those facts or its consideration is affected by legal or factual errors, the protestor must also show that the agency's lack of meaningful consideration or its legal or factual errors were prejudicial.[69] This likely means that, in a protest of a solicitation or award involving CMMC requirements, the protestor would likely have to show that the alleged unmitigated OCI tainted the CMMC requirements in a manner that was prejudicial to the protestor.

3. Competition

DOD is required by statute and regulation to provide for full and open competition in soliciting offers and awarding government contracts unless one or more exceptions applies.[70] None of these statutory or regulatory exceptions would appear to justify less than full and open competition in the case of a solicitation imposing a particular CMMC maturity level as a minimum requirement for contract award. The imposition of such minimum requirements will necessarily reduce the field of offerors able to compete and may result in an increase in solicitations that draw only a single eligible offeror, especially in the early days of the CMMC program when companies and their subcontractors are still in the process of becoming certified. DOD may be faced with situations where it would need to delay its procurement if it considers it important that there be several eligible offerors.

In addition, DOD's imposition of CMMC levels may generate bid protests. Designated CMMC levels might be challenged by offerors or would-be offerors as a minimum requirement that is unreasonable or that unduly restricts competition. Conversely, it is conceivable that an offeror with a relatively high-level CMMC accreditation might contend that the specified CMMC maturity level is too low for DOD's actual needs for the procurement, thereby seeking to reduce the field of competitors.

Successfully protesting the minimum CMMC level requirement that DOD chose to impose in a particular procurement would likely be difficult unless that requirement was clearly wide of the mark. Agencies are given great discretion in selecting evaluation factors, including "go/no go" evaluation factors. Such factors will not be disturbed unless they are arbitrary or in violation of procurement statutes or regulations. This is particularly true of a factor imposed by DOD to further national security, including cybersecurity. For example, in Oracle's protest of DOD's solicitation for the JEDI cloud services contract, the Court of Federal Claims found that the solicitation's Gate Criteria 1.2, which required offerors to have no fewer than three physical existing unclassified data centers within the U.S. that supported at least one Infrastructure-as-a-Service (IaaS) offering and one Platform-as-a-Service (PaaS) offering that are FedRAMP Moderate "Authorized" at the time of proposal submission, was reasonably tied to DOD's minimum security needs for the processing and storing of its controlled unclassified information.[71]

In a further holding relevant to CMMC-based protests, the Court of Federal Claims rejected Oracle's argument that Gate Criteria 1.2 represented a "qualification requirement" subject to the provisions of 10 U.S.C. § 2319, and that DOD had failed to comply with those provisions. The court noted that a qualification requirement is "a requirement for testing or other quality assurance demonstration that must be completed by an offeror before award of a contract," and is generally a "qualified bidders list, qualified manufacturers list, or qualified products list."[72] The court distinguished qualification requirements from "specifications," which it defined as "the requirements of the particular project for which the bids are sought, such as design requirements, functional requirements, or performance requirements."[73] Applying the relevant case law to the facts before it, the court concluded that the FedRAMP Moderate Authorization requirement was a specification rather than a qualification requirement, and therefore did not have to meet the statutory criteria for the use of such requirements. This decision will increase the burden on parties protesting a

solicitation's CMMC requirements on the grounds that such requirements constitute excessive or unjustified "qualification requirements," unless the protestor is able successfully to distinguish the CMMC requirements from the FedRAMP Moderate Authorization requirement at issue in the Oracle decision (or that decision is reversed on appeal.)

Finally, the Court of Federal Claims rejected Oracle's argument that the FedRAMP Moderate Authorization gateway criterion transformed the procurement into one that used other than competitive procedures in violation of CICA's and the FAR's full and open competition requirement. The court noted the Federal Circuit's statement in *National Government Services, Inc. v. United States*, 923 F. 3d 977, 985 (2019), that "a solicitation requirement (such as a past experience requirement) is not necessarily objectionable simply cause that requirement has the effect of excluding certain offerors who cannot satisfy that requirement." The court also found that agency emails and statements that Oracle pointed to as evidencing the agency's intent to limit the number of bidders "are insufficient to demonstrate that the agency is using 'other than competitive procedures' in the JEDICloud procurement."[74] Instead, the court found that "the agency structured this procurement to use full and open competition and the gate criteria are just the first step in the evaluation of proposals."[75] Again, unless it is overturned on appeal, the Oracle decision will make it more difficult to protest an agency's imposition of a CMMC-based "go/no go" evaluation factor unless the protestor is able to draw meaningful distinctions between such a factor and the FedRAMP Moderate Authorization gate criterion at issue in *Oracle*.

The chances of successfully protesting an agency's use of CMMC levels as a gateway evaluation factor would likely be greater if the offeror or potential offeror challenged not the reasonableness of the CMMC "go/no go" evaluation factor itself, but rather DOD's potentially uneven or arbitrary application of that factor in a particular procurement. Thus, for example, a decision by a DOD program office that the proposed subcontractors of one offeror would be required to be certified at CMMC Level 3 while CMMC Level 1 sufficed for another offeror's subcontractors could be challenged on the grounds of disparate treatment. Alternatively, one offeror's access to non-public information regarding the maturity levels (or lack thereof) of another offeror's proposed subcontractors could form the basis of an unequal access to non-public competitive OCI. (See Section 2 above.)

Some contractors may also turn to bid protests as a way to challenge perceived problems with the CMMC certification process. For example, an offeror who believes that a competitor was wrongly credited with a certain CMMC maturity level might seek to challenge that accreditation through a protest. Whether the GAO or Court of Federal Claims would find such issues to be valid grounds for a protest and within their jurisdiction remains to be seen and likely depends on a number of factors, including whether there is another forum in which such grievances could be head. These and other potential grounds for protest of awards based upon minimum CMMC maturity level requirements will be explored in a forthcoming article on CMMC and bid protests by Akin Gump lawyers Bob Huffman and Tom McLish.

Finally, CMMC maturity levels could also be considered matters of contractor and subcontractor responsibility. If so, it remains to be seen whether CMMC certification at a particular level will be considered sufficient to demonstrate the contractor's or subcontractor's responsibility concerning cybersecurity capabilities.

Furthermore, it is unclear whether DOD contracting officers will be free to consider cybersecurity-related factors other than CMMC certifications, including an offeror's past or present compliance with DFARS-7012 or past or present data breaches, in making determinations of contractor responsibility or non-responsibility. The interaction of CMMC certifications and responsibility determinations will be explored in greater detail in the forthcoming article on CMMC and bid protests.

D. Conclusions

Implementation of the CMMC program in all or most DOD contracts will have major impacts on the costs, competitiveness, and ethical pursuit of such contracts. As such, CMMC promises to have a profound impact of the government contracting process and community.

[1] Title 48 Code of Federal Regulations (CFR) Part 252.204-7012 (2020), https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

[2] See DOD, Cybersecurity FAQs, *Q1: When is DFARS clause 252.204-7012 required in contracts? Is the clause required in contracts for commercial items? Commercially available off-the-shelf (COTS) items?*, https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs (last accessed May 22, 2020).

[3] DFARS -7012(a) and (b).

[4] *Id*. -7012(a).

[5] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[6] DFARS -7012 (b)(2)(ii)(A).

[7] *Id*. -7012(a).

[8] *Id*. (emphasis added).

[9] *See id*. -7012(c).

[10] *Id*. -7012(a).

[11] *Id*.

[12] *See id*. -7012(a) and (c).

[13] *Id*. -7012(m)(1).

[14] *Id*. -7012(m)(2).

[15] See Shay D. Assad, DOD, Defense Pricing and Acquisition Policy, *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting* (Sep. 21, 2017), https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf; *see also* Exostar, *PIM Supplier Tips of the Month, October 2017: How do we benefit from the new NIST form?* (Dec. 6, 2017), https://exostar.atlassian.net/wiki/spaces/SEC/pages/173178886/October+2017+How+do+we+benefit+from+the+new+NIST+form.

[16] *See* Ellen Nakashima and Paul Sonne, *China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare* (Jun. 8, 2018), https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

[17] *See generally* U.S. Government Accountability Office (GAO), *Weapons System Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Oct. 8, 2018), https://www.gao.gov/products/GAO-19-128; GAO, *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, GAO-20-241 (Apr. 13, 2020), https://www.gao.gov/assets/710/705886.pdf.

[18] *See generally* DOD Office of the Inspector General, *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*, DODIG-2019-105 (Jul. 25, 2019),

https://www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-controlled-unclassified-information-on-contractor-ow/.

[19] See generally, U.S. Senate Committee on Armed Services, *Hearing: Cybersecurity Responsibilities of the Defense Industrial Base* (Mar. 26, 2019), https://www.armed-services.senate.gov/hearings/19-03-26-cybersecurity-responsibilities-of-the-defense-industrial-base.

[20] James Geurts, DOD, *Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks* (Sep. 28, 2018), http://thecgp.org/images/ASN-SIGNED-IMPLEMENTATION-OF-ENHANCED-SECURITY-CONTROL.pdf.

[21] *See, e.g.*, Samuel Greaves, Memorandum for All MDA Prime Contractors Through the Cognizant Contracting Officers (Jan. 12, 2018) https://www.the-center.org/getattachment/Our-Services/Cybersecurity-Services/Cybersecurity/DOD-CYBER-BEST-PRACTICES.pdf.aspx?lang=en-US.

[22] *See* Jared Serbu, *DoD to debut new cyber assessment program for contractors in less than a year*, Federal News Network (Jul. 23, 2019), https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2019/07/dod-to-debut-new-cyber-assessment-program-for-contractors-in-less-than-a-year/; Nicole Ogrysko, *DoD unveils new cybersecurity certification model for contractors*, Federal News Network (Sep. 5, 2019), https://federalnewsnetwork.com/defense-main/2019/09/dod-unveils-new-cybersecurity-certification-model-for-contractors/.

[23] *See* DOD, Cybersecurity Maturity Model Certification (CMMC) (Version 1.02) at 1 (Mar. 18, 2020) (hereinafter CMMC Model Ver. 1.02).

[24] *Id*. at 2.

[25] *Id*. at 4.

[26] *Id*.

[27] *Id*.

[28] *Id*.

[29] *See id*.

[30] *Id*. at 5.

[31] *Id*. at 6.

[32] *Id*. at 6–7.

[33] *Id*. at 5.

[34] *See* Dwight Weingarten, *Arrington Says New CMMC Will Benefit Small Businesses*, MeriTalk (Mar. 30, 2020), https://www.meritalk.com/articles/arrington-says-new-cmmc-will-benefit-small-businesses/.

[35] *See* DOD, CMMC FAQs 20 and 21, https://www.acq.osd.mil/cmmc/faq.html (last visited May 25, 2020).

[36] *See* Connie Lee, *New CMMC Rules for Defense Contractors to Come in November*, National Defense Magazine (May 11, 2020), https://www.nationaldefensemagazine.org/articles/2020/5/11/new-cmmc-rules-for-defense-contractors-to-come-in-november.

[37] *See, e.g.*, DOD, CMMC FAQs 10 and 13.

[38] Katie Arrington, *Securing the DoD Supply Chain*, Slide 10 (presented at the American Conference Institute, Toronto, Canada, on Feb. 11, 2020).

[39] *See* CMMC FAQs 19 and 20; Jackson Barnett, *CMMC won't apply to commercial-off-the-shelf suppliers, DOD website shows*, Fed Scoop (May 5, 2020), https://www.fedscoop.com/cmmc-exemption-cots-suppliers/.

[40] Justin Doubleday, *Pentagon to give companies credit for exiting certifications under new contractor cybersecurity program*, Inside Cybersecurity (Apr. 1, 2020) ("We want to provide reciprocity for any government certifications that have been achieved by companies." (quoting Katie Arrington)), https://insidecybersecurity.com/daily-news/pentagon-give-companies-credit-existing-certifications-under-new-contractor-cybersecurity; *see also* Sara Friedman, *Tech-industry groups raise CMMC concerns on FedRAMP*

reciprocity, vulnerability disclosures, Inside Cybersecurity (Mar. 30, 2020), https://insidecybersecurity.com/daily-news/tech-industry-groups-raise-cmmc-concerns-fedramp-reciprocity-vulnerability-disclosures.

[41] *See, e.g.*, CMMC Model Ver. 1.02 at 2 ("When implementing CMMC, a [Defense Industrial Base] contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s), depending upon where the information to be protected is handled or stored.").

[42] *See, e.g.*, Daniel Wilson, *DOD Cybersecurity Rollout May Be Delayed by COVID-19*, Law360 (May 22, 2020), https://www.law360.com/articles/1276271/dod-cybersecurity-rollout-may-be-delayed-by-covid-19.

[43] *See id.*; see also DOD, Press Release, DOD Signed Memorandum of Understanding with Cybersecurity Maturity Model Certification Accreditation Board (Jun. 1, 2020) ("The [DOD] intends to conduct CMMC Pilots with new contracts this year. The requests for information (RFIs) associated with these pilots will be released this summer."), https://www.defense.gov/Newsroom/Releases/Release/Article/2204213/dod-signed-memorandum-of-understanding-with-cybersecurity-maturity-model-certif/.

[44] Office of Management and Budget, Pending EO 12866 Review, *Strategic Assessment and Cybersecurity Certification Requirements* (DFARS Case 2019-D041), https://www.reginfo.gov/public/do/eoDetails?rrid=130604; see also Sara Friedman, *Defense Dept. begins process of changing acquisition regulations for cyber certification program*, Inside Cybersecurity (June 1, 2020), ("COVID-19 is impacting the rule change, but Arrington said the pandemic is not changing the timeline for training and accreditation for auditors through the CMMC Accreditation Body or the upcoming release of requests for information from the Defense Department."), https://insidecybersecurity.com/daily-news/defense-dept-begins-process-changing-acquisition-regulations-cyber-certification-program.

[45] CMMC FAQ 18, https://www.acq.osd.mil/cmmc/faq.html.

[46] *See, e.g.*, Justin Doubleday, *Defense Dept. pushing to keep cyber certification costs to $1,000 per year for most companies*, Inside Cybersecurity (Apr. 17, 2020) ("[Arrington] said most companies will build CMMC costs into their labor rates . . . ."), https://insidecybersecurity.com/daily-news/defense-dept-pushing-keep-cyber-certification-costs-1000-year-most-companies.

[47] 48 C.F.R. Part 31.201-2 (2020), https://www.acquisition.gov/content/31201-2-determining-allowability.

[48] 48 C.F.R. Part 31.201-3 (2020), https://www.acquisition.gov/content/31201-3-determining-reasonableness.

[49] *Id*.

[50] *See, e.g.*, Marjorie Censer, *DOD acquisition leader Fahey: Pushback from industry over cost of CMMC 'upsets me a little bit'*, Inside Cybersecurity (Jan. 21, 2020) (" 'They're supposed to be there today,' he said of contractors cybersecurity, pointing to existing standards set by [NIST]."), https://insidecybersecurity.com/daily-news/dod-acquisition-leader-fahey-pushback-industry-over-cost-cmmc-upsets-me-little-bit.

[51] Jim Goepel, CMMC AB Board Member and Chair of Finance Committee, Comments at the American Bar Association's Cybersecurity, Privacy, & Data Protection Committee and its Acquisition Reform & Emerging Issues Committee: Understanding DOD's CMMC: Practical Considerations From Practitioners (Mar. 24, 2020), https://www.americanbar.org/groups/public_contract_law/committees/acquis/meetings/.

[52] 48 C.F.R. 31.201-4 (2020).

[53] *Id*.

[54] *See supra* note 46.

[55] 48 C.F.R. Part 31.202 (2020), https://www.acquisition.gov/content/31202-direct-costs.

[56] 48 C.F.R. Part 31.203 (2020), https://www.acquisition.gov/content/31203-indirect-costs. *See generally* 48 C.F.R. Parts 9904.401 and 9904.402 (2020); Defense Contract Audit Agency, Contract Audit Manual, Chapter 8 Cost Accounting Standards (Aug. 2019), https://www.dcaa.mil/Portals/88/Documents/Guidance/CAM/Chapter_08_-_Cost_Accounting_Standards.pdf?ver=2019-10-10-155312-227.

[57] *See generally* 48 C.F.R. Part 9904.402-50 (2020).

[58] 48 C.F.R. Part 31.109 (2020), https://www.acquisition.gov/content/31109-advance-agreements.

[59] *See* 41 U.S.C. § 3502(b).

[60] *See id.* § 3505(a).

[61] Cybersecurity Maturity Model Certification Accreditation Body, *Board Code of Ethics*, https://www.cmmcab.org/ethics.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *See, e.g.*, Sara Friedman, *Defense official: Auditors won't be allowed to consult for companies they certify under CMMC program*, Inside Cybersecurity (Apr. 30, 2020), https://insidecybersecurity.com/daily-news/defense-official-auditors-won%E2%80%99t-be-allowed-consult-companies-they-certify-under-cmmc.

[66] *Id.*

[67] *See* 48 C.F.R. Part 9.505 (2020), https://www.acquisition.gov/content/9505-general-rules.

[68] Inquiries, Inc., B-417415.2 (December 30, 2019).

[69] Id. at 5 ("Competitive prejudice is an essential element of a viable protest, and we will sustain a protest only where the protestor demonstrates that, but for the agency's improper actions, it would have had a substantial chance of receiving the award.").

[70] *See* Competition in Contracting Act ("CICA"), 10 U.S.C. § 2304, 41 U.S.C. § 3301; Federal Acquisition Regulation ("FAR") Part 6.1.

[71] Oracle America, Inc., v. United States, 144 Fed. Cl. 88, __, appeal pending, No. 19-2326; see also, Systems Analysis & Integration, Inc., B416899.2, –2019_CPD 15 (Jan. 2, 2019).

[72] *Id. Oracle*, 144 Fed. Cl. at 117– (quoting 10 U.S.C. § 2319(a)).

[73] *Id.* (quoting 10 U.S.C. § 2305(a)(1)(A)(i)-(B)(ii)).

[74] *See Oracle*, 144 Fed. Cl. at 119.

[75] *Id.*