ROGERS | JOSEPH | O'DONNELL

Overview & Analysis of DoD's CMMC Proposed Rule

By Robert Metzger, Stephen Bacon, Deborah Rodin, and Cindy Lopez
Mr. Metzger and Mr. Bacon are Shareholders; Ms. Rodin and Ms. Lopez are Associates of the Firm

I. INTRODUCTION

On December 26, 2023, the Department of Defense (DoD) published in the Federal Register the long-awaited Cybersecurity Maturity Model Certification (CMMC) Proposed Rule, which implements the CMMC 2.0 Program. 88 Fed. Reg. 89,058 (Dec. 26, 2023). Public comments are due on February 26, 2024. Also published on December 26, 2023 is a "Notice of Availability" of eight "guidance documents" for the CMMC model, assessments, scoping, and hashing.[1]

The Proposed Rule at Title 32 CFR Part 170 implements the CMMC Program, but additional rulemaking in the acquisition regulations at Title 48 CFR is needed to implement the CMMC program requirements for government contractors.[2] The CMMC 2.0 Program has three key features:

1. **Tiered Model**: CMMC requires organizations, and their subcontractors, that are entrusted with Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) to implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information.

2. **Assessment Requirement**: CMMC assessments allow DoD to verify the implementation of cybersecurity standards.

3. **Implementation through Contracts**: Once CMMC is fully implemented, certain DoD contractors handling FCI or CUI will be required to achieve a particular CMMC level as a condition of contract award.

88 Fed. Reg. at 89,058-59. Once the rulemaking is complete, DoD solicitations that involve the processing, storing, or transmitting of FCI or CUI on contractor systems will identify which CMMC level applies and which assessment type requirement must be met for contractors to be eligible for contract award.

The Proposed Rule describes the requirements for each CMMC level:

1. **CMMC Level 1.** Contractors and applicable subcontractors must verify, on an annual basis, through ***self-assessment,*** that all applicable "basic safeguarding" requirements of FAR clause 52.204-21 have been

[1] These guidance documents are available at CMMC Guidance Documents (regulations.gov).

[2] The Fall 2023 Regulatory Agenda, for RIN 0750-AK81, indicates that revisions to the Part 48 rules are to be produced, as a Notice of Proposed Rulemaking (NPRM), in March 2024.

implemented. Results of the self-assessment are to be submitted electronically in DoD's Supplier Performance Risk System (SPRS). There is an additional new "affirmation" requirement, also to be entered in SPRS, that a senior official from the prime contractor and any applicable subcontractor must annually affirm continuing compliance with the security requirements.

2. **CMMC Level 2.** Contractors and applicable subcontractors must verify, on a triennial basis, that all applicable security requirements of NIST Special Publication (SP) 800-171 Rev 2 have been implemented.

   a. **Self-Assessment.** Some contracts will require a self-assessment of the Level 2 security requirements, which must be entered electronically in SPRS.

   b. **Certification Assessment.** Other contracts will require a certified independent third-party assessment organization to verify the contractor's implementation of the Level 2 security requirements.

   Selected requirements are allowed to have a Plan of Action & Milestones (POA&M) that must be closed out within 180 days of the assessment. Level 2 also contains the "affirmation" requirement, described above, with the affirmation required after every assessment, including POA&M closeout, and annually thereafter.

3. **CMMC Level 3.** Contractors and applicable subcontractors must verify, on a triennial basis, through ***DoD assessment*** that all applicable security requirements of NIST SP 800-172 have been implemented, in addition to the requirements of CMMC Level 2. Selected requirements are allowed to have a POA&M that must be closed out within 180 days of the assessment. Level 3 also contains the "affirmation" requirement, described above, with the affirmation required after every assessment, including POA&M closeout, and annually thereafter.

The Proposed Rule describes, at §170.3(e), a roll-out in four phases, with DoD introducing CMMC requirements in solicitations over a three-year period. Notably, DoD will include ***self-assessment*** requirements "when warranted by the FCI and CUI categories associated with the planned effort" from "the effective date of the DFARS rule that will implement CMMC requirements." 88 Fed. Reg. at 89,071. DoD "intends to include CMMC requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026, when warranted by any FCI or CUI information protection requirements for the contract effort." *Id.* Before that time, however, DoD Program Managers will have discretion to include CMMC requirements in accordance with DoD policies. *Id.* How many PMs will avail themselves of that discretion, and why, remains to be seen.

II. HISTORY OF THE RULE

CMMC first grew out of the November 2010 Executive Order (E.O.) 13556, Controlled Unclassified Information. 88 Fed. Reg. at 89,058. This Order aimed to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls." The E.O. established the CUI Program to standardize the way the executive branch handles information requiring safeguarding or dissemination controls (excluding information that is classified under E.O. 13526, Classified National Security Information or any predecessor or successor order; or the Atomic Energy Act of 1954, as amended).

In 2019, DoD announced the development of CMMC as a way of verifying protection of sensitive unclassified information shared with contractors by the Department or generated by contractors, rather than relying on a "self-attestation" model of security.[3] In September 2020, DoD published an interim rule, Defense Federal Acquisition Regulation Supplement (DFARS): Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041). 85 Fed. Reg. 61,505 (Sept. 29, 2020). This implemented the DoD's initial vision for the CMMC Program ("CMMC 1.0") and outlined the basic features of the framework to protect FCI and CUI, i.e., tiered model of practices and processes, required assessments, and implementation through contracts.

The interim rule describing CMMC 1.0 became effective on November 30, 2020, establishing a five-year phase-in period. The interim rule resulted in approximately 750 public comments. In response, in March 2021, the Department initiated an internal review of CMMC's implementation. In November 2021, the Department announced "CMMC 2.0," a revised version of the program. After a lengthy gestation period, the newly published proposed rule followed.

III. INITIAL TAKEAWAYS

The proposed rule largely follows what DoD has announced and described as the expected CMMC 2.0 content. Notably:

- DoD clearly has decided that small and innovative businesses must be protected, and most such businesses, when holding CUI, will be subject to Level 2 independent, third-party assessment requirements.

- DoD is managing the burden, in part, by a slow rollout and by means (yet to be fully explained) to decide which solicitations will be subject to the CMMC Level 2

[3] Contributing to this decision, we believe, was the 2018 MITRE "Deliver Uncompromised" Report, which states, at 38: "Beyond trusting contractors to provide 'adequate security' as required by DFARS 252.204-7012, the Department can establish measures and methods to review and assess actual accomplishment of promised security measures."

certification assessment obligations, and when the requirements will be included in which solicitations.[4]

- If anyone was expecting a "wholesale" dilution of obligations for small businesses, it is not present. There is expressed sensitivity for the challenge for small businesses, but threat concerns, as well as potential impacts of compromise, explain the decision to retain a "high bar" for most DoD suppliers, including small businesses, who handle CUI.[5] Impacts upon and cost risks for small businesses are discussed below, at pp. 8-9.

- Much of the rule endorses the activities of The Cyber AB, while obliging it to meet various standards not presently met. *See* Proposed Rule § 170.8. Many activities presently undertaken by the AB, are "ratified" in the sense they now appear in proposed 32 CFR regulations, at Subpart C – CMMC Assessment and Certification Ecosystem.

- It is noteworthy how much authority the proposed regulation confers to the current "DoD-authorized Accreditation Body," which, as recognized in the proposed regulation, is doing business as the Cyber AB. 88 Fed. Reg. at 89,120. This is a function of scale, i.e., the very large number of defense suppliers subject to the rule (at levels 1, 2, and 3), and the limitations of the Department's resources.[6]

- For example, it will be the C3PAOs and the Cyber AB, not DoD, that is responsible to resolve disputes as to whether an organization has met, or not met, individual security requirements.[7] Negative decisions could affect contractor eligibility for

---

[4] Proposed Rule § 170.5 (Policy) assigned to program managers, and requiring activities, the responsibility to determine the CMMC Level that will apply to a procurement. Factors to be considered include but are not limited to: (1) criticality of the associated mission capability; (2) type of acquisition program or technology; (3) threat of loss of the FCI or CUI to be shared or generated in relation to the effort; (4) potential for and impacts from exploitation of information security deficiencies; and (5) other relevant policies and factors, including Milestone Decision Authority guidance.

[5] The Proposed Rule explains that "CMMC is focused on securing the Department's supply chain, including the smallest, most vulnerable innovative companies." 88 Fed. Reg. at 89,102.

[6] *See* 88 Fed. Reg. at 89,083. "Given the size and scale of the DIB, the Department cannot scale its existing cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors and subcontractors every three years. The Department's existing assessment capability is best suited for conducting targeted assessments for the relatively small subset of DoD contractors and subcontractors that support designated high-priority programs involving CUI." *Id.*

[7] There may be disputes between an Organization Seeking Certification (OSC) and its Certified Third-Party Assessment Organization (C3PAO), or conceivably between the OSC and/or the C3PAO and the

new awards. As proposed, assessments could avoid judicial review. Whether this is sufficient to withstand a legal challenge, on the grounds that an inherently governmental function is improperly delegated to a private sector entity, is subject to further review and consideration.

- A positive development is the treatment of "operational technology" (OT) and related technologies, especially relevant to manufacturing, such as SCADA, PLC, and the like. The Proposed Rule states that OT, and related assets, are to be "documented ***but are not assessed***" against other CMMC security requirements. 88 Fed. Reg. at 89,066; *see also* Table 1 to § 170.19(c)(1). Assessors are to "Review the SSP" but are not to "assess against other CMMC security requirements." While this solves the mis-fit of CMMC requirements to OT, it does not recognize much less address the distinct and significant security issues of OT and other assets in these categories.

- Most of the attention of the defense industry has been pointed towards the Level 2 CMMC requirements, which reflect the 110 controls imposed by NIST Special Publication (SP) 800-171. The proposed regulation indicates that DoD anticipates 139,201 companies will be subject to Level 1 self-assessment over the contemplated 7-year phase-in period. This is approximately twice as many companies as those DoD expects to be subject to Level 2 (4,000 self-assess, and 76,598 subject to certification (third-party) assessment, for a total of 80,598). While Level 1 requires a *self*-assessment, against the 15 basic safeguarding requirements of FAR 52.204-21, the proposed regulation is very clear that the Level 1 self-assessment cannot be performed informally; rather, it "must be performed using the objectives defined in in NIST SP 800-171A … for the security requirement that maps to the CMMC Level 1 security requirement". Proposed Rule § 170.15(c)(1)(i). It is doubtful that these demands are presently recognized by even a small fraction of the companies with FCI subject to Level 1.

IV. OBSERVATIONS

A. Applicability

1. FCI & CUI

In general, CMMC applies to defense contractors that process, store, or transmit either FCI or CUI. FCI "means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government." 48 C.F.R. § 4.1901; *see* Proposed Rule § 170.4

Accreditation Body (the AB), but DoD would not be a party to these as the proposed rule is drafted. *See* 88 Fed. Reg. at 89,070.

(using 48 C.F.R. § 4.1901 definition for FCI).[8] The CMMC Program requirements for Level 1 will apply when the contract effort requires contractors to process, store, or transmit FCI on its unclassified information system. 88 Fed. Reg. at 89,069.

CUI includes "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." 32 C.F.R. § 2002.4(h); *see* Proposed Rule § 170.4 (using 32 C.F.R. § 2002.4(h) definition for CUI).[9] If CUI is processed, stored, or transmitted on a contractor information system, a higher level of CMMC compliance or certification is required. 88 Fed. Reg. at 89,069. The CMMC Level required to protect CUI (i.e., CMMC Level 2 Self-Assessment as described in § 170.16, CMMC Level 2 Certification Assessment as described in § 170.17, or CMMC Level 3 Certification Assessment as described in § 170.18) is determined by the Department based upon the sensitivity of the CUI and will be identified in the solicitation. *Id.*

2. Subcontract Flowdown Requirements

CMMC Level requirements will apply to any subcontractors throughout the supply chain at all tiers that will process, store, or transmit FCI or CUI on contractor information systems in the performance of the subcontract. Prime contractors will be required to identify the applicable CMMC Level for each subcontract depending on the type of information the subcontractor will process, store, or transmit and the CMMC Level requirement in the prime contract. In some cases, the prime and subcontractor will be subject to different CMMC Levels.

If the subcontractor will handle FCI, the subcontract will be subject to Level 1. When the subcontractor will handle CUI, it will be subject to at least a Level 2 Self-Assessment but will be required to have a Level 2 Certification Assessment if the prime contract includes that requirement. If the prime contract requires a Level 3 Certification Assessment, the rule states that a CMMC Level 2 Certification Assessment will be the minimum requirement. It is unclear whether or under what circumstances a subcontractor would be subject to a Level 3 Certification Assessment.

---

[8] Excluded from this definition is "information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments." *Id.*

[9] CUI, however, "does not include classified information . . . or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency." *Id.*

3. Foreign partners

In the Proposed Rule, DoD noted several comments concerning foreign partners. DoD was asked, for example, "if international subcontractors of a U.S. prime will require CMMC certification" and "if there is a strategy for legally implementing CMMC requirements beyond the U.S. DIB." 88 Fed. Reg. at 89,068. While DoD reportedly is working with foreign governments on reciprocal security arrangements, the Department's position, in the Proposed Rule position, is that all prime and subcontractors must comply with these requirements:

> Contractors are required to comply with all terms and conditions of the contract, to include terms and conditions relating to cybersecurity protections and assessments. In addition, offerors will be required to comply with the pre-award CMMC requirement. This holds true when a contract clause is flowed down to subcontractors …This rule makes no distinction about which C3PAOs may assess which companies seeking certification.

Id.[10]

Very likely, and understandably, the Department seeks assurance that foreign participants in the DoD supply chain, when provided with CUI, must act to accomplish the same level of security as DoD demands of its U.S. suppliers. While there are undoubtedly inter-governmental measures that can address this risk, DoD cannot accommodate lesser security as this would be tantamount to acquiescence in penetration of international supply chain participants, by foreign sources, with results harmful to U.S. national security.

B. Administration

1. Roles and responsibilities

Proposed Rule Part 170, Subpart B sets forth DoD's and the Cyber AB's roles and responsibilities. The Office of the Department of Defense Chief Information Officer (DoD CIO) Office of the Deputy CIO for Cybersecurity (DoD CIO(CS)) provides oversight of the CMMC Program and will be responsible for establishing CMMC assessment, accreditation, and training requirements as well as developing and updating CMMC Program policies and implementing guidance. Proposed Rule § 107.6(a).

The CMMC Program Management Office (PMO), within the DoD CIO, is responsible for the granting and revocation of the validity status of the appropriate

[10] Note that the Proposed Rule requires C3PAOs to undergo a FOCI risk assessment and can potentially be disqualified for FOCI. § 170.9(b)(5).

CMMC certification level, including investigating and acting upon indications that an active CMMC Self-Assessment or CMMC Certification Assessment has been called into question.[11] Proposed Rule § 170.6(a)-(b). The PMO is authorized to revoke the validity status of the appropriate existing CMMC Self-Assessment(s) or CMMC Final Certification Assessment(s), if any results of the investigation demonstrate non-compliance. *Id.* § 170.6(c).

The DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is responsible for:

- Conducting CMMC Level 3 Certification Assessments and uploading assessment results into the CMMC instantiation of eMASS (DoD's Enterprise Mission Assurance Support Service);
- Issuing CMMC Level 3 Certification Assessment certificates;
- Conducting CMMC Level 2 assessments of Cyber AB and prospective C3PAOs information systems that process, store, and/or transmit CUI;
- Creating and maintaining a process for assessors to collect the list of assessment artifacts and upload artifact data into the CMMC instantiation of eMASS;
- As authorized and in accordance with all legal requirements, entering and tracking, appeals and updated results arising from CMMC Level 3 Certification Assessment activities into the CMMC instantiation of eMASS; and
- Performing a Level 2 Certification Assessment every three years of the Cyber AB.

Proposed Rule §§ 170.7(a), 170.8(b)(6).[12]

[11] While what is sufficient to call an assessment result "into question" is unclear, this language does not appear to mean that DoD will adjudicate disputes as to whether a C3PAO properly declines to issue a certification assessment; on these, after review within the C3PAO, and escalation to the Accreditation Body, the "decision of the Accreditation Body will be final." Proposed Rule § 170.8.

[12] Proposed Rule § 170.16(c)(2)(iii) provides that a Cloud Service Provider (CSP) may satisfy security requirements "equivalent to those established by the FedRAMP Moderate (or higher) baseline." Presently unstated is the role of DIBCAC, if any, or, the Cyber AB, for that matter, in providing guidance as to what establishes equivalence. This important question must be addressed.

The Accreditation Body, presently the Cyber AB, is responsible for authorizing and ensuring the accreditation of CMMC C3PAOs in accordance with ISO/IEC 17020:2012 and all applicable authorization and accreditation requirements:

- Accredit C3PAOs who meet all requirements set forth in § 170.9 to grant CMMC Level 2 Certification Assessments and issue certificates of assessment;
- Identify all prospective C3PAOs to the CMMC PMO. The CMMC PMO will sponsor the prospective C3PAO for a FOCI risk assessment conducted by the DCSA using the SF 328 as part of the authorization and accreditation processes;
- Notify prospective C3PAOs of the CMMC PMO's eligibility determination resulting from the FOCI risk assessment;
- Establish, maintain, and manage an up-to-date list of authorized and accredited C3PAOs on a single publicly accessible website and provide the list of these entities and their status to the DoD through submission in the CMMC instantiation of eMASS;
- Provide the CMMC PMO with current data on C3PAOs, including authorization and accreditation records and status in the CMMC instantiation of eMASS. This data shall include the dates associated with the authorization and accreditation of each C3PAO; and
- Provide the DoD with information about aggregate statistics pertaining to operations of the CMMC Ecosystem to include the authorization and accreditation status of C3PAOs or other information as requested.

§ 170.8(b)(6).

In turn, the C3PAOs are responsible for uploading into the CMMC instantiation of eMASS assessment data, issuing certificates of assessments, and resolving appeals regarding Level 2 certification assessments. § 170.9(b), as discussed below.

2. Ethics, conflicts, and C3PAO obligations

The Proposed Rule, at § 170.8(b)(17) prohibits "CMMC Ecosystem" members "from participating in the CMMC assessment process for a CMMC assessment in which they previously served as a consultant to prepare the organization for any CMMC assessment." Proposed Rule § 170.9(b)(2) requires that C3PAOs must "[c]omply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in § 170.8(b)(17); and achieve and maintain compliance with ISO/IEC 17020:2012 (incorporated by reference, see § 170.2) within 27 months of authorization." The Accreditation Body is to develop policies for Conflict of Interest, as well as a Code of

Professional Conduct, and Ethics, that comply with specified ISO/IEC requirements – as well as requirements that DoD may impose. Proposed Rule § 170.8(b)(17); *see also* 88 Fed. Reg. at 89,064.

Each C3PAO is required to have a time-bound, internal appeals process to address disputes related to perceived assessor errors, malfeasance, and unethical conduct, consistent with ISO/IEC 17024:2012, or subsequent revisions. Proposed Rule §§ 170.9(b)(20), 170.10(b)(8). Organizations seeking certifications can request a copy of the process from their C3PAO. 88 Fed. Reg. at 89,070. Requests for appeals will be reviewed and approved by individual(s) within the C3PAO not involved in the original assessment activities in question. If a dispute regarding assessment findings cannot be resolved by the C3PAO, it will be escalated to the Cyber AB. The decision by the Cyber AB will be final. § 170.8(b)(16); § 170.9(b)(20).

3. Reporting and use of assessment results

DoD's Supplier Performance Risk System (SPRS) will function as DoD's official source for CMMC certification levels, which will allow DoD to confirm eligibility for award and ensure compliance during contract performance. DoD notes that "assessment results are documented in SPRS to enable contracting officers to verify the validity status of an offeror's certification level and currency (i.e., not more than three years old) prior to contract award." 88 Fed. Reg. at 89,078.

SPRS is based on inputs from the organizations themselves, C3PAOs, and/or DCMA DIBCAC. Proposed Rule § 170.6(a).

For CMMC Level 1, organizations submit the results of their annual self-assessments in SPRS and include the information required under § 170.15(a)(1).

CMMC Level 2 self-assessment results are similarly submitted to SPRS by the organizations themselves and must include the information required under § 170.16(a). However, CMMC Level 2 certification assessments, which are done through C3PAOs, are submitted by the CP3AO into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS. § 170.17(a)(1). Those submissions must include the information required under § 170.17(a)(1)(i).

CMMC Level 3 assessment results are submitted by the DIBCAC into the CMMC instantiation of eMASS and are automatically transmitted to SPRS. Those submissions must include the information required under Section 170.18(a)(1)(i).

C. Impacts

1. Small Business impacts

Over a seven-year period, DoD anticipates that approximately 164,000 small businesses will be required to comply with CMMC requirements. 88 Fed. Reg. at 89,085. While a substantial majority (63%) of those companies will only be subject to Level 1, nearly 60,000 small businesses will be subject to Level 2 and more than 1,300 will be subject to Level 3. Notably, DoD estimates that a very high percentage of these – roughly 57,000 small businesses –will be subject to Level 2 and will be required to pay an C3PAO to conduct a Certification Assessment to verify compliance with the security requirements outlined in NIST SP 800-171 Rev 2. This may prove burdensome for those companies in the DIB who have -7012 DFARS requirements but have not yet acted to satisfy these security requirements. However, as the Proposed Rule points out, the DFARS cyber obligations have required implementation, where the clause is present in contracts already taken, since Dec. 31, 2017, and, "therefore, the costs of implementing the security requirements for CMMC Levels 1 and 2 should already have been incurred and are not attributed to this rule." 88 Fed. Reg. at 89,087.

As compared to CMMC 1.0, DoD has taken some steps in CMMC 2.0 to reduce the compliance burden on small businesses. As expected, a 3PAO assessment is not required for Level 1 compliance, as DoD instead will accept contractor self-assessments. Moreover, during the initial implementation phases, DoD will have some discretion to permit Level 2 Self-Assessments in lieu of a Level 2 Certification Assessment conducted by a C3PAO.

While DoD provides tables with implementation timing, and costs, DoD's proposed "ramp up" period for Level 2 ends rather quickly. In Phase 1 (0-6 months), although DoD has discretion to require a Level 2 Certification Assessment, the rule states that DoD intends to require a Level 2 *Self*-Assessment as the condition for award. But by Phase 2 (6-18 months), DoD intends to require a Level 2 Certification Assessment as a condition for award and it only has discretion to delay that requirement to an option period. *See* Proposed Rule § 170.3(e) (discussion of "phased approach"). Absent other measures to assist small businesses who lack needed resources – financial, technical, and personnel – we anticipate many comments will likely urge DoD to lengthen the "ramp up" period for Level 2. Some may urge relief from some SP 800-171 requirements, permission to have more open Plans of Action & Milestones (POA&Ms), or other forms of greater latitude in being permitted to contract with less than full compliance. Very likely, DoD has considered these positions already. Worth note is the statement that: "The value of DoD's sensitive information (and impact of its loss to the Department) does not diminish when it moves to contractors - prime or sub, large or small." 88 Fed. Reg. at 89,069.

2. Cost of Compliance

Contractors that are subject to a Level 2 Certification Assessment will experience the most substantial cost impact due to the new requirements to hire and pay

an independent 3PAO and then to close out POA&Ms within the prescribed period of the initial self-assessment. *See* § 170.16(a)(ii)(A), (B). DoD estimates that small businesses will incur more than $100,000 for each Level 2 Certification Assessment, which must be completed every three years. This estimate includes only the cost of assessment because, as mentioned above, DoD assumes that contractors have already incurred the cost to implement security requirements mandated by existing DFARS clause 252.204-7012. The validity of DoD's cost estimates and underlying assumptions will be a subject of intense scrutiny during the public comment period.

DoD recognizes that, for firm-fixed price contracts, the cost of CMMC implementation will be reflected in a contractor's competitive price. If all contractors, small and large, are treated equally in the imposition of these requirements, then the risk is reduced of market discrimination, either against those who already comply, or those who now act and spend to comply. DoD also acknowledges that the cost of compliance may be recoverable as an allowable cost for cost-type contracts in accordance with existing FAR cost principles. But DoD specifically states that it "currently has no plans for separate reimbursement of costs to acquire cybersecurity capabilities or a required cybersecurity certification that may be incurred by an offeror on a DoD contract." 88 Fed. Reg. at 89,070. In other words, contractors may be able to recover ongoing CMMC compliance costs after award (likely via indirect cost allocation), but there is no apparent mechanism for contractors to recoup *pre-award* costs incurred to meet CMMC contract eligibility requirements.[13] DoD is likely opposed to paying such costs, now, for requirements that date back six or more years. The fiscal impacts could be significant, given the tens of thousands of companies which, conceivably, might seek reimbursement, and DoD has many other spending priorities.

3. Cloud & Managed Services

There has been confusion and concern as to how cloud services providers (CSP), and other external services that reside on or are delivered by the cloud, will be treated in the CMMC framework regulations. The Proposed Rule does not resolve these questions, though it avoids imposing obligations that would have been impossible to implement – such as requiring FedRAMP[14] Moderate for all cloud and cloud-based third-party service offerings.

The Proposed Rule provides that "CMMC does not offer comprehensive acceptance of FedRAMP" but does accept FedRAMP environments "in some cases" to

[13] The rule identifies resources available through the DoD Office of Small Business Programs and NIST's Manufacturing Extension Partnership programs that provide compliance resources and funding assistance options. 88 Fed. Reg. at 89,069.

[14] The FedRAMP program is a Federal Government-wide initiative that provides a standardized approach to security authorizations for cloud service offerings.

meet CMMC requirements for Cloud Service Providers. 88 Fed. Reg. at 89,070. When a contractor uses an external CSP to process, store, or transmit CUI or to provide security protection for any component, the CSP must either (i) be authorized as FedRAMP Moderate (or higher) on the FedRAMP Marketplace or (ii) meet security requirements "equivalent to" FedRAMP Moderate.

It is positive that "equivalency" is retained, as an alternative to enduring the large costs and long time required for formal FedRAMP authorization. What is missing, however, is sufficient guidance on how CSPs, or ESPs using cloud, are to meet the equivalency requirement. Nor is it clear how such third-party service providers, who do not have DoD contracts themselves, are to be eligible for a CMMC Level 2 (or higher) assessment.

According to the Proposed Rule, to demonstrate equivalency, CSPs are required to provide "a body of evidence (BOE) that attests to and describes how the CSP's product or service offering meets the FedRAMP baseline security requirements." 88 Fed. Reg. at 89,070. The Proposed Rule at § 170.16(c)(2)(ii) uses notably *different* wording, as it states:

> Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control ***that maps to the NIST SP 800–171 Rev 2*.**

(Emphasis added). What is perplexing is that FedRAMP Moderate requires satisfaction of 325 controls from NIST SP 800-53, in contrast to the 110 controls that are required, by SP 800-171, to protect CUI.

The rule likely needs improvement, or collateral actions need to be taken by the Cyber AB, possibly working with the private sector, to reconcile the apparent inconsistencies within the Proposed Rule. Service providers need a workable basis to assert, determine, and demonstrate equivalency, for assessors to validate such claims, and for prospective customers (who are organizations seeking assessment or certification) to receive the "inheritance" benefits of certified Cloud Service Offerings or External Services that rely upon cloud.

Presumably, the Cyber AB, with the involvement of DIBCAC, and with DoD's approval, could develop a "parallel" mechanism for the assessment and validation of "equivalency." This implies, however, decisions on which FedRAMP requirements should apply to protection of CUI possessed or used by commercial organizations. These need not, and should not, be identical to the 325 controls that are derived from NIST SP 800-53 for FedRAMP Moderate. Also, a new curriculum will be needed for training and

certification of assessors, capable of deciding "equivalency." Another objective should be to "qualify once" services and service providers who achieve "equivalency" so that this hurdle need not be imposed repeatedly.

Another area of perplexing and unsatisfying treatment concerns Managed Service Providers (MSP) or Managed Security Service Providers (MSSP). The Proposed Rule defines an External Service Provider (ESP)—which it identifies as a "CMMC-custom term"—as:

> external people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and / or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.

§ 170.4.

When a contractor uses an ESP other than a CSP, for CMMC Level 2, the ESP must have a CMMC Level 2 Final Certification Assessment. § 170.19(c)(2). This reflects, undoubtedly, DoD's concern that a service provider who assists many companies to satisfy CMMC Level 2 requirements itself should be demonstrably secure. Whether MSPs and MSSPs should be subject to all the same requirements, from SP 800-171, or the same assessment processes, from SP 800-171A and the corresponding CMMC Level 2 Assessment Guide, is not self-evident. Forcing MSPs and MSSPs into complete compliance with a NIST Standard that was not developed for such service providers could be problematic in process, costs – and results. As above, the eligibility of MSPs, or MSSPs, for a conditional or final Level 2 certification assessment is not established, since they provide services to companies under contract to DoD and are not themselves under DoD contracts.

The demands of CMMC, and other IT operation and cyber defense measures, have caused many tens of thousands of DIB companies to move towards CSPs, CSOs, and ESPs including MSPs and MSSPs. It is **essential** and **urgent** to take further and better measures to enable DIB suppliers, at all assessment levels, to use these services – *but* it is also important to recognize and act upon the different assurance needs that attach to service providers and offerings that affect multiple clients.