February 26, 2024

Via email: www.regulations.gov

John Sherman
Chief Information Officer
Office of the Chief Information Officer
Department of Defense
Washington, DC 20301

Re: Proposed Rule, Cybersecurity Maturity Model Certification (CMMC) Program; Docket ID: DoD-2023-OS-0063 (*Federal Register*, December 26, 2023)[1]

Dear Mr. Sherman:

Our associations welcome the opportunity to comment on the Department of Defense's (DoD's) proposed rule on the Cybersecurity Maturity Model Certification (CMMC) Program (aka CMMC 2.0).

OVERVIEW

The CMMC Program would establish new and significant mechanisms to assess defense (sub)contractors' compliance with security measures to safeguard sensitive, unclassified DoD information—specifically, Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)—that is processed, stored, or transmitted on contractor information systems. In particular, the requirements to protect CUI are established in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 Rev 2.[2] The CMMC Program would also create three levels or means of verifying contractors' compliance via self-assessments, third-party assessments, or government assessments.

We do not attempt to address the multiple elements raised in DoD's proposed rule. Rather, this letter consists of feedback from private entities, which ranges from high level to specific, that our groups have received on the CMMC Program. In general, industry feedback cuts across three categories—calls for more **clarity** (e.g., definitions), concerns about **costs**, and questions regarding **capacity**—and addresses additional process and organizational issues.

[1] https://www.federalregister.gov/documents/2023/12/26#defense-department

[2] According to the proposed rule, the CMMC Program consists of three progressive levels, each containing security requirements taken directly from existing regulations and guidelines. § 170.14(2) defines CMMC Level 1 as the 15 requirements listed in the FAR clause 52.204–21(b)(1). § 170.14(3) defines CMMC Level 2 as the 110 requirements from the NIST SP 800–171 Rev 2. § 170.14(4) defines CMMC Level 3 as 24 selected requirements from the NIST SP 800–172. *Federal Register* (*FR*), p. 89065.

CLARITY

Addressing ongoing and fundamental CUI questions. DoD contractors of all sizes have continuing, yet fundamental, questions about CUI, which is an umbrella term for all unclassified information that requires safeguarding under Executive Order 13556. A governmentwide CUI Registry provides information on the specific categories and subcategories of information that the executive branch guards closely.[3] Still, the scope of CUI marking is a leading concern that our associations consistently hear from contractors, and it should be a central one that DoD and industry spend more time working through.

It seems that DoD marks some digital and physical documents as CUI, but contractors are largely responsible for determining whether sensitive, unclassified information in their possession (e.g., paper documents) is CUI. Despite the availability of government aids and related materials to coach contractors on CUI, the level of uncertainty that businesses have expressed to us is too high. DoD and industry must have mutual recognition of what is or is not CUI if the CMMC Program is to get off the ground. DoD leadership should feel similarly and work with contractors to remedy businesses' queries.

The CMMC Program should only apply to CUI that is subject to a DoD contract and that CUI provided to contractors by non-DoD agencies should be subject to the requirements of those agencies and not the CMMC Program. Also, any information created in the normal course of business operations, such as in the electric subsector, should not automatically be considered inside the scope of CUI.

An industry group told our associations that "it's important to make these distinctions because DoD's existing requirements for safeguarding for CUI (i.e., DFARS 252.204-7012) are explicitly limited to information in support of a defense contract. In contrast, the proposed rule adopts, seemingly without any limits, the National Archives and Records Administration's [NARA's] definition of CUI, which applies to all CUI regardless of the agency in which it is connected."

The issue is not necessarily what DoD would enforce but what contractors may be effectively compelled to implement if the proposed rule is finalized in its current form. Absent a modest, but key, clarification from DoD, defense contractors may face penalties under the False Claims Act because the proposed rule requires attestation that NIST SP 800-171 security controls are in place for CUI, including perhaps beyond a defense contract. Some contractors may feel pressure to take a risk-adverse approach to safeguarding data and apply costly controls to all apparent CUI whether or not it is associated with DoD.

The industry group noted that "contractors with a CMMC Level 2 Certification Assessment requirement may find that their C3PAO [CMMC Third-Party Assessment Organization] strictly interprets the CMMC and assesses NIST SP 800-171 security requirements across all government CUI, whether or not it is associated with a DoD contract. If DoD intends

[3] https://www.archives.gov/cui

that the proposed rule only applies to DoD-related CUI, then it can avoid confusion in the future by making this 'DoD-only' distinction more explicit."

DoD can create confusion when it infers that contractor information can be deemed CUI because it matches general descriptions in the CUI Registry. However, our associations believe that there must be a specific basis in (1) statute, as with export controls or (2) a contract, as with Controlled Technical Information (CTI). Indeed, the CUI Registry should be revised to make this stipulation more plainly understood. It is also worth pointing out that CUI is an assortment of many different designations with different policy and legal justifications for its applicability. CUI can include both marked information provided by the government and information "that an entity creates or possesses for or on behalf of the government."[4] One constant with CUI is that it is not easy to identify unless a document is clearly marked at CUI.

In addition, the industry group said that "the point at which information is 'created' or 'possessed' by a contractor compared to developed in the normal course of operation for any customer is often uncertain, especially outside of the traditional defense industrial base. This problem can be especially acute for interconnected industries like electric utilities where, at least notionally, any information associated with the electric grid could implicate any consumer, public or private. Without clarification that the CMMC Program only covers CUI specifically subject to a defense contract, the proposed rule could assert control over practically any utility's data simply because DoD buys electric services from that utility."

This is not what the CMMC Program is intended to do, but some in industry believe there is a lack of clarity that needs to be remedied. After all, the CMMC Program's broad grant of authority would run contrary to the spirit of NARA's CUI definition adopted in DoD's proposed rule, which states that "CUI does not include . . . 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."[5]

Further, the industry group said, "DoD can avoid confusing many contractors by stating that the protection of CUI and any related (self)assessments or certifications are only subject to DoD oversight. DoD procedures require that the Defense Department affirmatively identify contractor information that it wants designated as CTI. DoD should work with contractors in each sector to provide clear guidance on the types of data that it considers CTI. Parties in industry have met with DoD representatives on a number of occasions to discuss defining and marking CUI. These discussions need to continue. Indeed, guidance that DoD provides to the electricity subsector sometimes generates more, not less, confusion. Our constituents would welcome a dialogue with DoD to clearly identify what information constitutes CTI and/or CUI, including the costs of applying heightened safeguards to this information."

---

[4] *FR*, p. 89080.

[5] "Controlled Unclassified Information (CUI)" is defined in 32 CFR 2002.4(h). *FR*, p. 89121. https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002/subpart-A/section-2002.4#p-2002.4(h)

In sum, some crucial questions regarding CUI that our associations consistently receive from members are:

- Will additional materials (e.g., sector-specific guidance) be provided to contractors? Materials that have been published to date do not seem to meet contractors' needs. Our associations appreciate that DoD is planning to work with industry on identifying and marking CUI proficiently, which is a step in the right direction.

- Which agencies besides DoD will mark information as CUI? Contractors are urging DoD to provide a clear and consistent definition of CUI to implement the CMMC Program.

- How does DoD plan to ensure that all organizations within the department, including the service branches,[6] will employ the same approach to identifying and marking CUI?[7]

Aligning Security Protection Data (SPD) with NIST cybersecurity definitions. Under the proposed rule, DoD creates a new term, SPD, which is used to partially define when an External Service Provider (ESP) is covered under the CMMC Program. A company told our associations that "SPD is neither defined in the proposed rule nor in the CMMC Program glossary (CMMC glossary). SPD is lightly referenced only three times in the proposed rule."

> *External Service Provider (ESP)* means 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** [bolding added] (*e.g.*, log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term)[8]

Also, SPD is not defined in the NIST cybersecurity resource center glossary (NIST glossary). The company said, "The closest term is 'security-relevant information,' which is defined as 'Information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.' Under the proposed rule, SPD would create ambiguity when an ESP is in scope for an assessment. This ambiguity would create confusion, if not conflict, when the conformity of ESPs is evaluated by an Organization Seeking Assessment (OSA), a C3PAO, and the DCMA's [Defense Contract Management Agency's] Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), which conducts CMMC Level 3 Assessments."

---

[6] https://www.defense.gov/Resources/Military-Departments

[7] See the U.S. Chamber's November 30, 2020, letter to DoD on CMMC 1.0, including on industry's uncertainty about CUI (pp. 2–3).
https://www.uschamber.com/assets/archived/images/11-30-20_uscc_letter_cmmc_final_version_1.0.pdf

[8] *FR*, p. 89121.

The company suggested that "to better ensure the harmonization of terms and the standardization of certain cybersecurity practices across the federal IT compliance landscape, we recommend that DoD adopt NIST's definition of 'security-relevant information' and include it in the CMMC glossary."

Clarifying Security Protection Assets (SPAs) and SPD to make scoping less difficult. A number of commercial entities that conduct business with the public and private sectors are concerned about new CMMC Program terms that go beyond FCI and CUI. DoD has seemingly created whole categories of data (i.e., SPAs and SPD) that cut against DoD's assumption that FCI and CUI can be readily identified and safeguarded.

More specifically, the proposed rule refers to SPAs as "assets providing security functions or capabilities to the OSA's CMMC Assessment Scope," whether or not these assets process, store, or transmit CUI. The proposed rule calls SPAs a "CMMC-custom term."[9] Neither the SPAs definition nor SPD are linked to NIST SP 800–171 Rev 2 controls. SPAs and SPD are not sufficiently defined within the proposed rule and could result in a significant broadening of the system boundaries associated with the CMMC Program.[10]

The proposed rule says that "prior to a CMMC assessment, the OSA must define the CMMC Assessment Scope . . ., representing the boundary with which the CMMC assessment will be associated." Yet such boundary-setting activities would prove difficult if key terms in the proposed rule, especially because SPAs and SPD are imprecise and can leave a contractor essentially guessing what is to be in-scope for an assessment.

11. CMMC Assessment Scope

Comment: **Multiple commenters requested details on assessment boundaries and what systems are in-scope for a CMMC assessment.** [Bolding added.] Questions included how assessment boundaries are defined, how networks composed of federal components (including systems operated on behalf of the government) and non-federal components are addressed, how centralized security services are treated, and how "enduring exceptions" are handled.

Response: § 170.19 states that **prior to a CMMC assessment, the OSA must define the CMMC Assessment Scope for the assessment, representing the boundary with which the CMMC assessment will be associated. This section includes detailed guidance on how to define the CMMC Assessment Scope**, [bolding added] how different categories of equipment are defined to be in- or out-of-scope for an assessment, how the security of specialized equipment is expected to be managed, External Service Providers considerations, and the incorporation of people, technology, and facilities into the boundary.

GFE [government furnished equipment], IoT [internet of things], OT [operational technology], and, as defined, Restricted Information Systems and Test Equipment are categorized as "Specialized Assets" in

[9] *FR*, p. 89122.

[10] Ibid.

§ 170.19. NIST SP 800–171 Rev 2 uses the term "enduring exceptions" to describe how to handle exceptions for Specialized Assets.[11]

A business said, "These custom terms—SPAs and SPD—add to the universe of data, albeit vaguely, that must be accounted for in the CMMC Program. Among other things, they go beyond the data that is outlined in Defense Federal Acquisition Regulation Supplement (DFARS) 52.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting." The business added, "Complicating matters, both SPAs and SPD would, per the proposed rule, need to meet the requirements for protecting CUI information 'irrespective of whether or not these assets process, store, or transmit CUI.' In short, what are contractors to make of terms that are weakly defined? It's a recipe for costly CUI confusion."

In addition, a private entity added, "As it stands, some SPAs can process, store, and transmit CUI, while other SPAs do not but are still classified that way, requiring the same level of protection as CUI. Most global companies do not classify security data using SPAs and SPD and neither do assessors that certify against existing international standards and FedRAMP [Federal Risk and Authorization Management Program], or NIST-related, standards."

Our associations believe that SPAs and SPD should be clarified such that they only need to meet the requirements for CUI when they process, store, or transmit CUI.

Refining the relationship between an External Service Provider (ESP) and a Cloud Service Provider (CSP). The CMMC Program refers to an ESP as "external people, technology, or facilities that the organization utilizes, including [CSPs], Managed Service Providers [MSPs], Managed Security Service Providers [MSSPs], [and] Cybersecurity-as-a-Service Providers."[12] Also, the CMMC Program refers to a CSP as "an external company that provides a platform, infrastructure, applications, and/or storage services for its clients."[13]

A firm told our associations that "the relationship between an ESP and a CSP is insufficiently clear because the proposed rule solely focuses on CSPs that 'process, store, or transmit' CUI.[14] But not all CSPs meet this description. The proposed rule does not specify anything about CSPs that solely provide security protection services (e.g., a cybersecurity firm) and do not handle FCI or CUI." The firm added that "this ambiguity creates a space where not all CSPs that should be in scope are addressed. Given that the definition of a CSP includes an 'external company' with the 'people, technology, or facilities that an organization utilizes' and provides comprehensive IT and/or cybersecurity services, it appears that a CSP is just a subset of

[11] *FR*, p. 89071.

[12] *CMMC Glossary and Acronyms*, version 2, December 2021, p. 4.

[13] The proposed rule cites the Cybersecurity and Infrastructure Security Agency et al. *Cloud Security Technical Reference Architecture*, version 1, August 2021, p. 41. *FR*, p. 89121.

[14] *FR*, p. 89066.

an ESP. We recommend that DoD refine the definition of a CSP to state that all CSPs are a specific type of ESP."

Relatedly, an industry group told our associations, "DoD should clarify the definitions of ESP and CSP to accommodate access by small and midsize businesses (SMBs). It is a fact that a high percentage of SMBs already look to MSPs, MSSPs, and other ESPs to manage their networks, handle data and information system security, and respond to cyber incidents. As drafted, the proposed rule could be read to apply FedRAMP Moderate cloud-security requirements to many of these ESPs. Few of the tens of thousands of SMBs would be able to afford third-party services if limited to those available today or in the near future with FedRAMP Moderate credentials."

The industry group added that "overly strict limits could force some SMBs to return to internal measures to protect on-premises systems, which cuts against the grain of today's leading cybersecurity practices. This, too, assumes that such SMBs have the resources (e.g., financial, human, and technical) to satisfy the CMMC Program requirements. Overly broad exclusion of ESPs, MSPs, and MSSPs could harm these valuable elements of the broader cybersecurity marketplace in the unintended pursuit of 'turning back the clock.'"

Another issue worth spotlighting is that the proposed rule says if an organization utilizes an ESP, other than a CSP, the ESP must have a CMMC Level 2 Final Certification Assessment. Left unexplained is how such service providers are to be assessed, or by whom, if they are not government contractors and therefore do not receive DoD contracts with the DFARS clause 252.204–7012. If the intention is for the Cyber AB to establish the needed mechanism, we believe that this should be explained.

> (2) If the OSA utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment. 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. If using a CSP for Level 2 Self-Assessment, see § 170.16(c)(2). If using a CSP for Level 2 Certification Assessment, see § 170.17(c)(5).[15]

Improving the definition of contractors' risk-based security policies, procedures, and practices. The phrasing regarding a "contractor's risk-based security policies, procedures, and practices"[16] and its variants is not defined within the proposed rule and supporting documentation. A company told our associations, "Given that this wording is used within the context of scoping assets to be evaluated under a CMMC assessment, it adds considerable uncertainty. Compared to this phrasing, NIST SP 800-171 Rev 2 defines a 'security domain' as a

[15] *FR*, p. 89134.

[16] *FR*, p. 89134.

'domain that implements a security policy and is administered by a single authority,' which is critical for determining a CMMC Assessment Scope."[17]

The company said, "It is unclear whether this is (1) the same 'security domain' that oversees a contractor's covered information system or (2) the assets under the auspices of the 'Contractor's risk-based security policies, procedures, and practices' operate outside of a contractor's covered information system 'security domain'?" The company added that "this confusion creates a potential disconnect for an OSA and a C3PAO that may assess them. If the assets operate under a separate security domain, then they are (per NIST SP 800-171 Rev 2) considered external to the boundary and would create a problematic overlap when they are described in a contractor's system security plan [SSP] and supporting documentation." On the contrary, the company noted, "If the assets fall under the covered contractor's information system security domain as specified by the SSP,[18] then it is unclear why this distinction is added only to 'Contractor Risk Managed Assets' and 'Specialized Assets.'"

Further, the company said, "Owing to the places where the phrase (i.e., a 'contractor's risk-based security policies, procedures, and practices') is implicated, an OSC [Organization Seeking Certification] is still required to describe its implementation within the SSP and supporting documentation—thus, the phrase seems congruent to a security domain. DoD should clarify the relationship between NIST SP 800-171 Rev 2 and the pending Rev 3 definition of 'security domain' and 'contractor's risk-based security policies, procedures, and practices.'"

The company concluded that DoD should improve the definition of "contractors' risk-based security policies, procedures, and practices" by newly adding the following definition to its CMMC glossary:

Security Domain

A management domain that implements a security policy and is administered by a single authority over all in-scope assets. A security domain is the OSA's risk-based security policies, procedures, and practices used to implement NIST SP 800-171 security requirements and other DoD-provided instructions, memorandums, and supplementary information. A security domain is documented in the SSP reflecting that domain.

Source: CMMC-custom term based on NIST SP 800-171

[17] See section 1.1, "Purpose and Applicability," pp. 2, 58.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

[18] "*System Security Plan (SSP)* means the formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan, as defined in CNSSI 4009 (incorporated by reference, see § 170.2)." *FR*, p. 89122.

Providing additional guidance on Level 2 and Level 3 assessment requirements. Our associations urge DoD to provide contractors with additional guidance on Level 2 and Level 3 assessment requirements. The *CMMC Level 2 Assessment Guide* provides guidance for conducting CMMC assessments for Level 2. For a contractor to achieve CMMC Level 2 certification, it must demonstrate achievement of all Level 1 and Level 2 practices. DoD says that guidance for conducting a CMMC Level 3 assessment is expected to be published at a later date.

- Prior to conducting a CMMC assessment, the contractor must specify the CMMC Assessment Scope. A CMMC assessment is the procedure used to certify that a contractor is compliant with the CMMC Level 2 standard.

- Contractors requiring a CMMC Level 2 certification must have a CMMC Level 2 assessment conducted by a C3PAO authorized by the CMMC Accreditation Body. C3PAOs grant CMMC Level 2 certificates of assessment.

- CMMC Level 1 addresses the protection of FCI and encompasses the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21.

- CMMC Level 2 addresses the protection of CUI, which is defined by NARA. According to DoD, this level provides increased assurance to the department that a contractor can adequately protect CUI at a level commensurate with the risks and threats.

The proposed rule states that contracts would include either a CMMC Level 2 Self-Assessment requirement or a CMMC Level 2 Certification Assessment requirement to verify a contractor's implementation of the CMMC Level 2 security requirements. The proposal notes that some requirements allow for a Plan of Action & Milestones (POA&Ms) that must be closed within 180 days of the assessment. Further, a Level 2 Self-Assessment must be performed on a triennial basis.[19]

A firm said that it would be constructive for "DoD to provide further criteria governing whether a Level 2 contract falls under the self-assessment or certification categories. The proposed regulation notes that decisions are ultimately driven by the sensitivity of the CUI involved, but the proposal and the assessment guide do not provide enough transparency into the types of data that would drive the type of assessment that DoD would require. This is particularly important for entities as they evaluate their existing contracts and/or prepare budgets to implement future CMMC Program requirements."

The firm noted that "the government has existing frameworks in place for the evaluation of various categories of data that are used to inform the level of security pertinent to certain information systems, such as those noted in NIST SP 800-60.[20] This publication is probably

[19] *FR*, p. 89060.

[20] https://csrc.nist.gov/pubs/sp/800/60/v1/r1/final
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf

familiar to contractors that work with other federal agencies under FISMA [the Federal Information Security Management Act] and FedRAMP. It also provides an appropriate level of guidance around multiple categories of information and the baseline cybersecurity requirements for safeguarding such data. The apparent absence of criteria and guidance in the proposed regulation opens the door to inconsistencies in how requirements are applied across applicable contracts."

The firm requested "more clarity regarding the types of CUI that would require enhanced protection against Advanced Persistent Threats (APTs) at CMMC Level 3. In the absence of guidance enabling contractors to distinguish between Level 2 and Level 3 requirements, there is the added concern that different DoD agencies could apply different certification requirements to a service offered by the same contractor."

Our associations believe that there is a significant difference between being in the Level 2 group that requires a certification assessment and being in the much smaller group that must self-assess. Our associations urge DoD to clarify how it would determine which entities need only to self-assess. Until the CMMC Program is in operation for a number of years, DoD should increase the number of contracting entities that are subject to a Level 2 Self-Assessment. If DoD applied risk-based considerations, officials could more narrowly tailor the entities for which a Level 2 Certification Assessment is required. Indeed, this would relieve some pressure on roughly 77,000 entities[21] as well as address the looming problem that there will be far too few credentialed assessors for the number of contractors that would either seek or be required to have certification assessments.

In addition, we think that the proposed rule provides little insight into what criteria would be applied, or what process(es) would govern, the determination of when a solicitation or contract requires a Level 3 Certification Assessment. Level 3 is intended to provide better protection against APTs, but these advanced threats may potentially be directed at a much larger group of entities than the 1,487 entities[22] that DoD estimates would be subject to Level 3 obligations. It is widely understood that meeting security mandates of Level 3 is substantially more demanding and expensive than ones at Level 2. Even sophisticated companies need sufficient time to comply with federal mandates. DoD is urged to improve its explanation of what factors it plans to use in deciding when to require Level 3 obligations. Further, DoD may need to be more accommodating on implementation schedules as some aspects of Level 3 when required could take several years to accomplish.

Coordinating (self-)assessments and annual affirmations. A business told our associations that "the (self-)assessment requirements under the proposed rule are not sufficiently coordinated with the annual affirmation requirements. Under the proposed rule, contractors are required to provide annual affirmations, while Level 2 Certification and Level 3 Certification assessments are required on a triannual basis. This disconnect may potentially and unfairly increase contractors' exposure under the False Claims Act. As such, the timeline for both should align to the requirement to conduct assessments every three years. At a minimum, clarity is

[21] *FR*, p. 89085.

[22] Ibid.

needed to define what would qualify as a change significant enough to trigger a change in an annual affirmation."

The business added, "Importantly, an attestation applicable to a contractor's entire supply chain is not practical. It is not consistent with federal procurement principles as evidenced in the current FAR and DFARS clauses. DoD should refine the scope of the subcontractor attestation to contract principles by clarifying that prime contractors are accountable to vet the next lower-tier direct supplier with which it has privity of contract. The relevant DFARS on this point could be mandatory flow-downs through the contractor's supply chain."

Also, "The definition of 'senior official' should be described in a manner so that professionals who complete the work and are best positioned (in contrast to operational management) to attest to overall compliance with the CMMC program are able to complete or delegate signing the affirmation statement, which requires a contractor to attest that it has met the applicable CMMC security requirements."

> (1) *Affirming official.* All CMMC affirmations shall be submitted by the OSA senior official who is responsible for ensuring OSA compliance with CMMC Program requirements.[23]

COSTS

Enabling flexible implementation of CMMC Program requirements. According to the proposed rule, the defense industrial base, or DIB, consists of 221,286 entities. Of these, DoD expects that 76,598 will be subject to a Level 2 Certification Assessment, of which 56,789 (74%) are small businesses.[24] The complex CMMC Program would apply to all these entities. Our associations believe that it is essential that DoD builds in flexibility in the administration, application, oversight, and enforcement of the proposed rule. Such flexibility would benefit DoD and the thousands of businesses subject to the CMMC Program. The circumstances of every business differ. The CMMC Program contemplates applying one complex rule, with even more complex accompanying documentation,[25] to all these businesses.

Likely there would be many circumstances where one or another facet of cybersecurity compliance cannot be achieved affordably or without unacceptable disruption to an enterprise. And in many situations, relief from a formal requirement may be warranted, especially where a risk assessment shows that the cost of 100% compliance is high while the likelihood of harm is comparatively low. DoD should direct that CMMC Program assessors to use their professional judgments and not require them to seek the maximum evidence of compliance where there is evidence of sufficiency. Perfect is often the enemy of the good. Indeed, making the rule too rigid

---

[23] *FR*, 89136.

[24] *FR*, p. 89085.

[25] https://dodcio.defense.gov/CMMC/Documentation

risks a disconnect between the contracting community and DoD that could make compliance practically impossible for hundreds if not thousands of businesses in the DIB.

Accounting for contract changes. A private entity told our associations that "our members express concerns about having multiple contracts with DoD and the resulting cost considerations. Multiple contracts mean complexity, including differing CMMC Program requirements. Regardless of whether a contract requires a Level 2 or Level 3 certification, there are significant financial outlays made for each one. For example, a contractor may achieve Level 2 compliance, but an unexpected change in a contract could mean ramping up to Level 3 compliance. We fear that the increased costs to become Level 3 compliant may not be part of the original project cost, so any marginal costs would be borne by us, the contractors."

"Similar reservations about costs extend to FedRAMP," added the private entity. The proposed rule says that an OSA may use a FedRAMP Moderate or higher cloud environment to process, store, or transmit CUI in execution of a contract requiring a CMMC Level 2 (under certain circumstances).[26] Still, the private entity said that "there is apprehension among many contractors about the backlog of FedRAMP certifications. Despite policymakers' efforts to rapidly increase the size of the FedRAMP marketplace by offering multiple authorization structures, we're seeing certification timelines extend to more than half a year."

Avoiding harm to small defense contractors. Our associations believe that the proposed rule would discourage many small and disadvantaged businesses from bidding on DoD construction projects. We are concerned about the likely adverse economic impact of the CMMC Program on promoting (sub)contracting between small businesses in the construction industry and DoD. Moreover, the department's proposal may directly contravene Congress' often-expressed intent to promote federal procurement to small businesses.[27] In 1978, Congress amended the Small Business Act requiring all federal agencies to set percentage goals for awarding procurement contracts to small businesses.[28]

To further illustrate, the majority of the construction industry and the Associated Builders and Contractors' (ABC's) members are classified as small businesses. These businesses represent the backbone of the construction industry. Unfortunately, the proposed rule would likely exacerbate a trend of increasing federal regulations, including in the areas of federal procurement and cybersecurity, that have reduced small business participation in federal contracting. Small businesses have suffered a 60% decline in the number of firms awarded federal contracts from 2010 to 2020, according to Small Business Administration (SBA) data.[29]

---

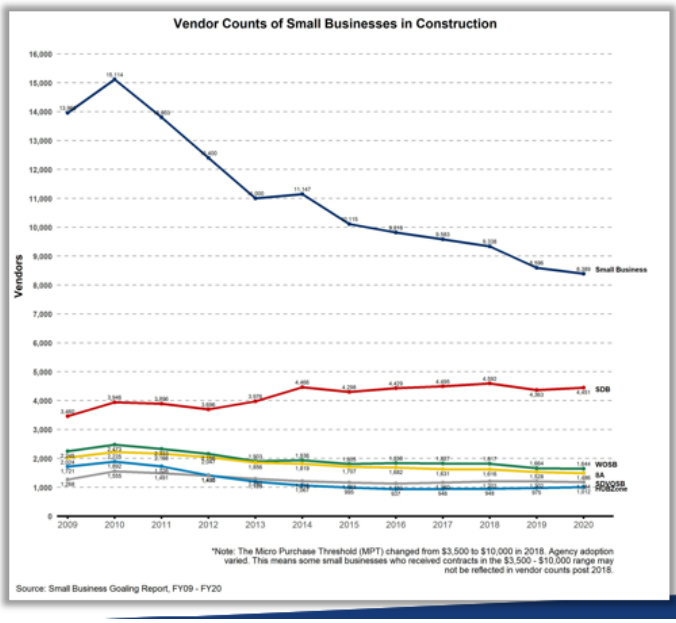
[26] *FR*, p. 89128.

[27] "An Overview of Small Business Contracting," Congressional Research Service, updated July 29, 2022. https://crsreports.congress.gov/product/pdf/R/R45576

[28] P.L. 95-507 (1978), 15 U.S.C. 644 (g).
https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1757.pdf
https://www.law.cornell.edu/uscode/text/15/644

[29] The chart in Appendix A is available at https://thetruthaboutplas.com/wp-content/uploads/2022/09/60-percent-decline-of-small-businesses-awarded-federal-construction-contracts-2010-to-2020.png. The data was prepared by an

Number of Construction Industry Small Businesses Awarded Federal Contracts Declined 60% From 2010-2020



Vendor Counts of Small Businesses in Construction

FY	Small Business	SDB	SDVOSB	HUBZone	WOSB	8A	SBGR
2009	13960	3460	1268	1721	2245	2024	16186
2010	15114	3946	1555	1892	2473	2225	17644
2011	13803	3896	1491	1726	2333	2168	16335
2012	12400	3696	1400	1416	2156	2047	14510
2013	11000	3976	1292	1199	1903	1856	12690
2014	11147	4466	1216	1067	1936	1819	12706
2015	10115	4298	1163	995	1805	1707	11724
2016	9818	4429	1133	937	1838	1682	12465
2017	9583	4495	1160	946	1827	1631	12146
2018	9338	4592	1202	948	1817	1616	11424
2019	8596	4363	1202	975	1664	1528	10504
2020	8389	4451	1184	1012	1644	1486	10191

The decline in small business participation in federal contracting directly correlates with increasing federal regulatory burdens. Surveys of ABC's membership have found that small business contractors often choose to bid on private sector and state or local government contracts that feature more regulatory clarity and less regulatory burdens, which mitigate expenses related to compliance.[30]

Our organizations are concerned that the proposed rule's imposition of a costly certification regime is likely to discourage competition from small contracting entities in the defense industry. The CMMC Program is likely to have a disparate impact on small business contractors and subcontractors, many of which are minority- and women-owned as well as disadvantaged businesses that employ a diverse workforce. Compared to many larger businesses, smaller construction firms are less capable of absorbing added regulations and costs.

SBA economist who said, "The charts represent data on vendors who have received obligations. The definition of 'small' comes from the contracting officer's determination when the contract was awarded. The COs [contracting officers] follow the NAICS size standards." Data is from the Federal Procurement Data System, which can be publicly accessed through SAM.gov.
https://sam.gov/reports/awards/standard

[30] "Survey: 97% of ABC Contractors Say Biden's Government-Mandated Project Labor Agreement Policies Would Make Federal Construction More Expensive," *ABC Newsline*, September 28, 2022.
https://www.abc.org/News-Media/Newsline/survey-97-of-abc-contractors-say-bidens-government-mandated-project-labor-agreement-policies-would-make-federal-construction-more-expensive

8. Small Business/Entities
A. ASSISTANCE/SUPPORT FOR SMALL BUSINESS

Comment: Several commenters suggested that in order to successfully implement cybersecurity requirements, contractors require support from the Department. One commenter suggested [that] DoD should perform an analysis of each requirement and ensure that necessary support structures are in place and fully functioning prior to implementing this rule, and that access to tech support/solutions should be provided. Multiple commenters suggested that more support and guidance [are] needed for small businesses trying to comply with CMMC. One commenter suggested that DoD should relax affiliation rules (in conjunction with the Small Business [Administration] (SBA)) to allow small companies to work together to meet CMMC requirements while spreading the cost over a larger base and expand mentor-protégé agreements for larger businesses to help smaller companies with CMMC appraisals.

One commenter expressed concern for non-traditional, innovative companies that are coming in through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) process and asked what DoD is doing to help them become compliant. Another noted that if CMMC Level 1 will be the minimum requirement for SBIRs and STTRs, regardless of whether they include FCI, it may significantly limit the number of universities that can partner with small businesses under these awards.

Response: DoD's Office of Small Business and Technology Partnerships (OSBTP) is working to provide SBIR/STTR programs with support for CMMC implementation through the use of Technical and Business Assistance. The SBA's affiliation rules are codified at 13 CFR 121.103, available at *https://www.ecfr.gov/current/title-13/chapter-I/part-121*. Any change to the SBA's affiliation rules is outside the scope of this rulemaking.[31]

The proposed rule states that DoD's Office of Small Business and Technology Partnerships (OSBTP) is "working to provide [Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR)] programs with support for CMMC implementation through the use of Technical and Business Assistance." While laudable, both data and practical experience tell our associations that such efforts would be insufficient toward enabling small businesses (sub)contractors to effectively bid on DoD construction projects.

Overlooking the costs of compliance for newly covered contractors under the CMMC Program. A business told our associations that DoD "should provide more clarity in the CMMC Program on the types of entities that are considered subcontractors under the proposed regulation." The CMMC Program uses the definition of "Subcontractor" in the *Code of Federal Regulations* (48 CFR 3.502-1)—

1) Means any person, other than the prime contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with such prime contract; and

[31] *FR*, p. 89069.

2) Includes any person who offers to furnish or furnishes general supplies to the prime contractor or a higher[-]tier subcontractor.[32]

The business added, "The definition, which is incorporated by reference, is overly broad. It suggests, for example, that a network of medical providers—many of which are small businesses—could be considered subcontractors under the proposed rule. While the scope of the data-centric CMMC Program is dependent on the handling of FCI and CUI, DoD needs to consider narrowing the proposal's scope or more vigorously pursue reciprocity between the CMMC Program and HIPAA [the Health Insurance Portability and Accountability Act of 1996]. Many entities are already covered under HIPAA, and the overlap between HIPAA and NIST SP 800-171 needs to be considered."[33]

In addition, the business said that "the extension of the CMMC Program to any subcontract down the entirety of a prime's supply chain has the potential to newly cover a significant number of private entities. Such an outcome helps explain industry concerns including the burdens that small businesses would shoulder to meet the proposed rule's requirements (e.g., the costs of pre-assessment consulting services and third-party assessments) and deadlines. DoD does not seem to account for small businesses that become newly covered under the CMMC Program."

The proposed rule says, "DoD did not consider the cost of implementing the security requirements themselves because implementation is already required [by the 2016 FAR clause 52.204–21 and the 2017 DFARS clause 252.204–7012] . . . 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** [bolding added]. As such, the nonrecurring engineering and recurring engineering costs to implement the security requirements defined for CMMC Level 1 and Level 2 are not included in this economic analysis."[34]

The business pointed out that "the department's estimation of public costs incorrectly assumes that all current and *potentially new* defense contractors have 'already' incurred the costs of complying with certain FAR and DFARS clauses. But a problem with this thinking is that new entrants to the defense contracting community may not have DoD's security requirements for handling CUI already baked into their cybersecurity operations. This seems to be a notable oversight of the proposed rule."

---

[32] *FR*, p. 89122.
https://www.law.cornell.edu/cfr/text/48/3.502-1

[33] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[34] *FR*, p. 89087.

CAPACITY

Reassuring contractors about public-private capacity for conducting assessments. The proposed rule states that DoD intends to include CMMC Program requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026. A company told our associations that "many contractors are distressed that the C3PAO community and DoD may lack sufficient capacity to conduct the number of assessments, particularly for Levels 2 and 3, which would be required in order to facilitate competition in government contracting." The company added that "despite DoD acknowledging the potential for future capacity issues, the proposed rule does not adequately address whether DoD is prepared to assess contractors that must undergo a Level 3 Certification Assessment[35] in order to bid on a contract."

> **D. MARKET CAPACITY FOR ASSESSMENTS**
>
> *Comment:* Multiple commenters wanted details about assessor availability and were concerned that a **lack of assessors would impact the schedule** [bolding added] for including CMMC requirements in solicitations and contractor planning to attain CMMC certification to meet those requirements.
>
> *Response:* The phased implementation plan described in § 170.3(e) is intended to address ramp-up issues, provide time to train the necessary number of assessors, and allow companies the time needed to understand and implement CMMC requirements. **An extension of the implementation period or other solutions may be considered in the future to mitigate any C3PAO capacity issues, but the Department has no such plans at this time.** [Bolding added.] If changes to the implementation plan occur, DoD policies that govern requirements definition in the acquisition process will be modified.[36]

The company said that "insufficient capacity for conducting Level 3 Certification Assessments could easily thwart the goals of the Competition in Contracting Act (CICA) of 1984 (41 U.S.C. 253)[37] by decreasing the total amount of eligible contractors in the defense marketplace. We believe that DoD should be in regular contact with industry on forecasting market supply and demand for Level 3 Certification Assessments. DoD needs to reassure industry that both public and private assessors are going to be ready to meet market demand."

Similarly, a business said that it "has concerns with the development of another federal C3PAO certification program. We are skeptical that there's going to be an adequate supply of FedRAMP-certified organizations that can meet the demand of CMMC-regulated contractors. It is well known that the FedRAMP-certification process is very slow, and it is likely to have a direct impact on DIB contractors and effective CMMC Program implementation."

---

[35] *FR*, p. 89060.

[36] *FR*, p. 89072.

[37] 41 U.S.C. 253.
https://www.govinfo.gov/app/details/USCODE-2009-title41/USCODE-2009-title41-chap4-subchapIV-sec253

In addition, the business said, "We share the apprehension of others regarding the ability of DoD to accredit the necessary number of assessment firms that would be required to meet the uptick in contractor demand for CMMC certifications. Our perspective is all the more salient because of the vast number of subcontractors in prime contractors' supply chains that could be newly covered under the CMMC Program but aren't part of DoD's projections."

ADDITIONAL PROCESS AND ORGANIZATIONAL ISSUES

Addressing additional process and organizational issues. DoD is urged to consider several key procedural and organizational recommendations (arranged alphabetically) that affect the department and contractors under the proposed rule.

- **Acknowledge the need for waivers.** Our associations appreciate that DoD is reluctant to open the door too widely to requests for waivers. But there are likely to be circumstances, perhaps more than presently anticipated, where waivers would be practically necessary (e.g., to avoid supply chain disruptions) if a key participant cannot meet certain requirements. Complex organizations may encompass many sectors or be integrated with many private entities, such that relief from formal CMMC Program requirements would be necessary on a whole-of-enterprise basis rather than for just one contract or one program. Our associations believe that more authority should be given to contracting officers to grant waivers. DoD should describe a process by which high-level acquisition or service officials may approve waivers when justified, including applying at an enterprise level.

Comment: **Many commenters were concerned about the lack of waivers or POA&Ms.** [Bolding added.] Several commenters commented that not allowing waivers is impractical and will impact the ability of businesses to qualify for contract award. Commenters asked for clarification on the differences between POA&M that are not allowed by CMMC and the plans of action as required in the CMMC Level 3 control (now CMMC Level 2 under CMMC 2.0), CA.2.159 (now CA.L2–3.12.2 under CMMC 2.0). Many noted that POA&Ms are necessary when managing activities like system upgrades, vendor changes, and company acquisitions to avoid temporarily falling out of compliance.

Response: Under certain circumstances, the CMMC Program does permit contract award to organizations that have an approved and time limited POA&M. See § 170.21 for additional information on POA&Ms. **There is no process for organizations to request waiver of CMMC solicitation requirements. DoD internal policies, procedures, and approval requirements will govern the process for DoD to waive inclusion of the CMMC requirement in the solicitation.**[38] [Bolding added.]

- **Allow contractors to use an alternative means of compliance vis-à-vis the stipulation that an ESP must have a CMMC certification level "equal to or greater than the certification level the OSA is seeking."** For instance, a firm noted, "A CMMC-certified contractor should have the option to use non-CMMC certified ESPs if the contractor

[38] *FR*, p. 89076.

retains the artifacts or documentation. This way the contractor can use this information to demonstrate to a CMMC assessor that such data is being managed by the ESP using the contractor's risk-based policies, procedures, and practices aligned with the relevant CMMC level."

> If an OSA utilizes an ESP, other than a Cloud Service Provider (CSP), the ESP must have a CMMC certification level equal to or greater than the certification level the OSA is seeking. For example, if an OSA is seeking a CMMC Level 2 Certification Assessment the ESP must have either a CMMC Level 2 Certification Assessment or a CMMC Level 3 Certification Assessment.[39]

- **Authorize a safe harbor vis-à-vis contractor compliance.** Our associations believe that a safe harbor should be a priority for DoD and the CMMC Program, which is consistent with the White House's *National Cybersecurity Strategy*. DoD is urged to ensure that contractors are protected from regulatory and legal liability when they meet the security requirements in accordance with the relevant CMMC Program levels.

- **Continue working with contractors to identify which data is CUI.** A business told our associations, "While a document that has already been marked as CUI by DoD or a higher tier contractor is relatively easy for contractors to identify as containing CUI, contractors need clear guidance on their contractual instructions on when data that they are creating in performance of a contract rises to the level of CUI. This is crucial for the success of the CMMC Program, which hinges on clear definitions of CUI."

  The business added, "After all, the proposed CMMC Program assumes that if it is determined that a single document containing CUI is present in a certain IT enclave, that could suddenly create a requirement for the enclave to be certified at CMMC Level 2 Certification Assessment. Therefore, it is important for contractors to have crystal clear instructions on whether the content they create counts as CUI. It is in DoD's interest for contractors to efficiently determine which environments must be certified to CMMC Level 2 or higher as well as reduce unnecessary confusion, compliance difficulties, and costs."

- **Enable zero trust as a solution to protecting CUI.**[40] A company urged DoD to "enable a zero trust solution as an appropriate, compliant approach for processing and properly safeguarding CUI data. A zero-trust approach would provide a higher level of security while also aligning with the intent and the overall direction of the CMMC Program."

---

[39] *FR*, p. 89066.

[40] "Zero Trust Architecture," NIST, August 10, 2020. https://www.nist.gov/publications/zero-trust-architecture

- **Establish an adjudication authority within DoD.** DoD has seemingly ceded much authority to the Cyber AB,[41] reflecting the scale of the certification challenge and the limitations of DoD's internal resources, including those of the DCMA DIBCAC. Our associations are concerned that key decisions, including ones affecting contractor eligibility for contracts, would be resolved by an external party, the Cyber AB, with no DoD involvement. DoD's office of general counsel should consider whether this is an acceptable delegation to the private sector of an inherently government function. Many in industry would be reassured if DoD established an adjudication resource within the department.

- **Examine the extent to which CMMC Program requirements should apply to its contractors.** A private entity said, "DoD should be mindful of the compliance burden it creates for a range of companies, including ones that provide physical goods to DoD or are small and midsize businesses. For companies where federal business does not account for a large share of their overall revenue—or that may not have extensive expertise with DoD's cybersecurity programs and rules—DoD should make a concerted effort to offset the costs and streamline processes for complying with the CMMC Program.

- **Increase the permissibility of POA&Ms.** A company said, "Under the proposed rule, the ability to rely on POA&Ms is overly constrained, particularly in the context of small businesses that often have comparatively reduced resources. Therefore, an overly restrictive POA&Ms model may have a disproportionate impact on small businesses. A phased model allowing a minimum of one-year PO&AMs for all controls for the first three years of the CMMC Program would ensure visibility to small business risk while moving toward full compliance."

  Also, an industry group recommended that DoD "permit extending an existing POA&Ms based on risk and where it is impracticable to meet the proscribed timeline."

> CMMC allows the use of a Plan of Action [&] Milestones (POA&Ms) for specified CMMC Level 2 and 3 security requirements. Each POA&M must be closed, *i.e.,* all requirements completed, within 180 days of the initial assessment.[42]

- **Reduce industry compliance costs by harmonizing CMMC Program requirements across the department.** According to an industry group, "CMMC requirements should replace similar but conflicting or redundant contracting requirements. This problem may apply only to our sector, including the United States Transportation Command, or TRANSCOM. But there are other examples worth exploring to advance regulatory harmonization and global operations with reciprocity" (see Appendix).

---

[41] https://cyberab.org

[42] *FR*, p. 89078.

- **Refrain from enabling "full access" to contractor information and information systems.** Per a separate yet related rulemaking, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the contracting agency should not be authorized to have "full access" to a contractor's information, information systems, and personnel in response to a (potential) "security incident."[43]

- **Use FIPS-compliant versus FIPS-validated encryption.** A firm told our associations, "To ensure that government processes are able to keep up with advancements in technology, government contractors should be required to use FIPS-compliant encryption as opposed to FIPS-validated encryption. (FIPS compliance refers to an application or product that is using Federal Information Processing Standard-approved encryption modules to protect data that is at rest on or transiting the application or product.)[44] This would enable equivalent protections while preventing stop gaps in industry and enable DoD to continue to meet its objectives."

Our associations thank you for the opportunity to provide DoD with comments on the CMMC Program. Private sector engagement is essential to bolstering the supply chain security of federal agencies. We look forward to working with DoD to help develop and implement the CMMC Program.

47G—Utah Aerospace and Defense Association
Alliance for Digital Innovation (ADI)
Associated Builders and Contractors (ABC)
BSA | The Software Alliance
Construction Industry Round Table (CIRT)
National Association of Wholesaler-Distributors (NAW)
National Utility Contractors Association (NUCA)
Power & Communication Contractors Association (PCCA)
Security Industry Association (SIA)
U.S. Chamber of Commerce

---

[43] DoD, General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) proposed rule, Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing, *FR*, October 3, 2023.
https://www.federalregister.gov/documents/2023/11/01/2023-24025/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing-extension
https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing

See the U.S. Chamber's comments on the proposed rule's "full access" provision on pp. 1–6 of our February 2, 2024, letter. Among other things, the letter states, "The Chamber strongly urges the government to step back from its unprecedented stance to authorize 'full access' to contractors' information and information systems. Policymakers should engage directly with industry before moving ahead with this significantly problematic provision." https://www.regulations.gov/comment/FAR-2021-0017-0062.

[44] "Compliance FAQs: Federal Information Processing Standards (FIPS)," NIST, last updated in November 2019. https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips

Appendix

DoD is urged to collaborate with the Office of the National Cyber Director on streamlining regulations and reciprocity. For several years, policymakers have wanted to "align, leverage, and deconflict" policies, laws, and regulations to increase U.S. cybersecurity through improved efficiency.[45] However, progress is still largely aspirational and domestically focused. Nonetheless, the CMMC Program would apply to international companies that manage global operations and platforms.

Depending on the service or type of products that DoD contractors offer, industry is likely subject to multiple requirements, assessments, and certifications across the federal government. Cloud service providers, for instance, are required to meet many conditions in DoD's *Cloud Computing Security Requirements Guide* and FedRAMP.

Our associations urge DoD to help policymakers and industry streamline existing cyber-related regulations to meet CMMC Program requirements. Our associations welcome the step taken by DoD under § 170.20 ("Standards acceptance"). The department states, "In order to avoid duplication of efforts" and reduce the aggregate cost to industry and the department, "OSCs that have completed a DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping will be eligible for CMMC Level 2 Final Certification Assessment" under certain conditions.[46] For many contractors, this is limited but welcome progress. Our associations appreciate that DoD has "reserved" space under § 170.20 to add more standards and so forth.

DoD says that its proposed rule would not duplicate, overlap, or conflict with its current information safeguarding requirements.[47] However, many in industry strongly disagree with this viewpoint. A key challenge facing both government and industry is that the CMMC Program adds to the total mix of contractors' federal enterprise risk management, incident reporting, and supply chain security obligations.[48]

Selected Excerpts From the Prosed Rule Related to DoD Cybersecurity Regulations and Standards

10. Acceptance of Alternate Standards

[45] See, for example, the Chamber's July 2016 letter to Cybersecurity Forum for Independent and Executive Branch Regulators. https://www.uschamber.com/sites/default/files/u.s._chamber_letter_to_cyber_forum_july_8_final.pdf

[46] *FR*, p. 89134.

[47] *FR*, p. 89077.

[48] For example, see "Software group urges OMB to lead harmonization effort on cyber regulations, artificial intelligence executive order mandates," *Inside Cybersecurity*, February 9, 2024. https://insidecybersecurity.com/daily-news/software-group-urges-omb-lead-harmonization-effort-cyber-regulations-artificial

A. NIST SP 800–171 REV 2 DOD ASSESSMENTS AND CMMC ASSESSMENTS

Comment: Multiple commenters asked for clarification on reciprocity between NIST SP 800–171 Rev 2 DoD Assessments and CMMC assessments.

Response: As stated in § 170.20(a), **DoD intends to allow qualified standards acceptance of High confidence assessment using NIST SP 800–171 Rev 2 for CMMC Level 2**. [Bolding added.] However, the CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses relating to cybersecurity assessments.[49]

B. CLOUD STANDARDS

Comment: Many commenters expressed concerns regarding CMMC recognition of Federal Risk and Authorization Management Program (FedRAMP) and requested guidance on which FedRAMP baselines, if any, would be granted standards acceptance at each CMMC Level. A few commenters sought assurance that DoD Cloud Computing Security Requirements Guide (SRG) Impact Levels 4 and 5 would not be applied to CMMC Level 3.

Response: **CMMC does not offer comprehensive acceptance of FedRAMP.** [Bolding added.] The CMMC Program allows the acceptance of FedRAMP environments in some cases to meet CMMC requirements in connection with use of a Cloud Service Provider (CSP). If an OSC uses an external CSP to process, store, or transmit CUI or to provide security protection for any such component, the OSC must ensure the CSP's product or service offering either (1) is authorized as FedRAMP Moderate or High on the FedRAMP Marketplace; or (2) meets the security requirements equivalent to those established by the Department for the FedRAMP Moderate or High baseline. The CSP will provide evidence that its product or service offering meets the security requirements equivalent to FedRAMP Moderate or High by providing a body of evidence (BOE) that attests to and describes how the CSP's product or service offering meets the FedRAMP baseline security requirements. Note that for any portion of the on-premises (internal) network that interacts with the cloud service offering and is within the CMMC Assessment Scope, the OSC is required to meet all applicable CMMC requirements to achieve certification.[50]

C. OTHER STANDARDS

Comment: Numerous commenters asked whether CMMC could leverage the results of other assessments, such as ISO/IEC 27001/27002, NIST SP 800–53, NIST SP 800–172, HITRUST, DoE Cybersecurity Capability Maturity Model, NIAP Common Criteria Testing Laboratory Services (CCEVS), Committee on National Security Systems (CNSS) Instruction No. 12533 (CNSSI 12533), ISA/IEC–62443, DoD's Security Technical Implementation Guides (STIG), NIST Cyber Security Framework (CSF), NIST Risk Management Framework (RMF), the American Institute of CPAs Service and Organizational Controls, Service and Organization Controls (SOC) Trust Services Criteria (SOC 2), ISA/IEC–62443, ITAR, Criminal Justice Information Services (CJIS) security standards, and non-ISO/IEC standards used by foreign partners such as the Australian Cybersecurity Centre Essential Eight Maturity Model.

---

[49] *FR*, p. 89070.

[50] *FR*, p. 89070–89071.

Response: The CMMC Program standards acceptance is defined in § 170.20 of this rule.[51]

---

23. Relationship to Existing Regulations

Comment: Several commenters asked about the implications of having DFARS clauses 252.204–7012 and 252.204–7021 coexist in contracts and wanted to know if all the 252.204–7012 requirements, including the requirements for "adequate security," incident reporting, and flow-down, apply in the presence of 252.204–7021. Others were concerned about a perceived conflict on the protection of CUI between NIST SP 800–171 Rev 2, which specifies the minimum requirements to provide "adequate security" for CUI on nonfederal systems and DFARS clause 252.204–7021 based on the CMMC Program. Multiple commenters wanted to know if the 252.204–7021 clause and the CMMC requirements override contractor responsibility to comply with other applicable clauses of the contract, or other applicable U.S. Government statutory or regulatory requirements. Others were concerned about a continued proliferation of security requirements.

Response: CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract, including DFARS clause 252.204–7021. As such, DoD cannot address applicability of or changes to current DFARS clause 252.204–7021 or other current DFARS cybersecurity provisions or clauses at this time.

DoD does not intend to impose duplicative cybersecurity protection or assessment requirements. [Bolding added.] There is no conflict between the CMMC cybersecurity protection requirements described in this rule and DoD's current information safeguarding requirements, including those set forth in DFARS clause 252.204–7012. This CMMC rule adds new requirements for the assessment of contractor implementation of underlying information security standards and guidelines, as applicable, such as those set forth in FAR clause 52.204–21 and in the NIST SP 800–171 Rev 2. This rule also prescribes additional information security protection and assessment requirements for CMMC Level 3, derived from NIST SP 800–172, for certain limited scenarios.[52]

24. Phase-Out of Existing Cybersecurity Requirements

Comment: Several commenters asked whether DFARS clause 252.204–7012, DFARS provision 252.204–7019 and 252.204–7020 will be phased out since DFARS clause 252.204–7021 is now a requirement.

Response: The CMMC Program requirements proposed in this rule will be implemented in the DFARS, as needed, which may result in changes to current DoD solicitation provisions and contract clauses, including DFARS clause 252.204–7021. As such, DoD cannot address applicability of or changes to current DFARS clause 252.204–7021 or other current DFARS cybersecurity provisions or clauses at this time.

The information safeguarding requirements and cyber incident reporting requirements set forth in DFARS clause 252.204–7012 will not be phased out as a result of this rule. CMMC Program

[51] *FR*, pp. 89070–89071.

[52] *FR*, pp. 89076–89077.

requirements provide DoD with verification, through self or third-party assessment, that defense contractors have, in fact, implemented DoD's cybersecurity protection requirements.

In addition, the requirements of this rule will not be fully implemented (and will not appear in all DoD contracts) until 2026 or later. As such, DoD will continue to require the current cybersecurity protections as reflected in the identified DFARS provisions and clauses for contracts that do not include a CMMC requirements.[53]

---

§ 170.20 Standards acceptance.

(a) *NIST SP 800–171 Rev 2 DoD assessments.* In order to avoid duplication of efforts, thereby reducing the aggregate cost to industry and the Department, OSCs that have completed a DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping will be eligible for CMMC Level 2 Final Certification Assessment under the following conditions:

(1) *DCMA DIBCAC High Assessment.* An OSC that achieved a perfect score with no open POA&M from a DCMA DIBCAC High Assessment conducted prior to the effective date of this rule, is eligible for a CMMC Level 2 Final Certification Assessment with a validity period of three (3) years from the date of the original DCMA DIBCAC High Assessment. Eligible DCMA DIBCAC High Assessments include ones conducted with Joint Surveillance in accordance with the DCMA Manual 2302–01 Surveillance. The scope of the CMMC Level 2 Final Certification Assessment is identical to the scope of the DCMA DIBCAC High Assessment. In accordance with § 170.17, the OSC must also submit an affirmation in SPRS and annually thereafter to achieve contractual eligibility.

(2) [Reserved]

(b) [Reserved][54]

[53] *FR*, p. 89077.

[54] *FR*, p. 89134.