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

February 26, 2024

Ms. Diane Knight
Acquisition and Rulemaking Lead
Cybersecurity Maturity Model Certification Program Office
U.S. Department of Defense

Electronic Submission: www.regulations.gov, Docket ID: DoD-2023-OS-0063

Re: Comments on the Proposed Rule for the Cybersecurity Maturity Model Certification (CMMC) Program

Dear Ms. Knight:

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide comments on the proposed rule for the second revision of the Cybersecurity Maturity Model Certification Program (CMMC 2.0).

NDIA is the nation's oldest and largest defense industry association, representing more than 1,700 corporate and over 65,000 individual members from small, medium, and large contractors, a majority of which are small businesses. Our members engage daily with the federal government's national and homeland security apparatuses. They are well-versed in the array of cybersecurity requirements and implementation challenges.

NDIA and its member companies are committed to securing the data and systems that power the defense industrial base (DIB), as well as the platforms, infrastructure, and services that support our nation's warfighters. Simultaneously, to avoid extraneous costs and burdens on industry, NDIA has been attentive to focusing resources and efforts to prioritize protecting the critical information and systems that truly matter.

NDIA fully supports the policy objectives of the CMMC program and has provided multiple comments on behalf of its members as the Department of Defense (DoD) formulated different iterations of the program. The CMMC proposed rule, however, presents a dramatic impact on the DIB as it imposes costs and stringent requirements for which compliance must be attested and/or independently assessed. Considering that the rule will rely heavily on DIB compliance and collaboration, NDIA would note that the short time frame to comment on the 234-page proposed rule published on December 26, 2023, diminishes the ability of industry to fully evaluate and respond to the proposal.

NDIA appreciates that the proposed rule addresses some of the recommendations previously provided by industry stakeholders to streamline the rule and improve clarity, which include reducing the number of compliance levels from 5 to 3, allowing Level 2 self-assessments for NIST SP 800-171, and applying Level 3 certification to a smaller number of contracts. Even though they are not defined within the rule, we applaud the DoD's recognition of Managed Security Providers (MSPs) and Managed Security Service Providers (MSSPs), both of whom play a critical role within the DIB cybersecurity ecosystem. Service providers are key to the success of the CMMC rollout, requiring critical differentiations between cloud

and security providers as their functionality and capability vary as to the applicability of standards and certifications.

NDIA also offers the following additional comments and recommendations on the proposed rule to address areas needing further improvement:

DoD Must Delineate Clear and Actionable CUI Marking Instructions and Responsibilities in Contracts as a Prerequisite for Success Under CMMC

It is impossible to understate how dependent the risk management goals of CMMC 2.0 are upon the ability of government and industry to effectively manage and safeguard defense-sensitive Controlled Unclassified Information (CUI). Effective management, however, is only possible with clear, accurate identification of what information requires protection and consistent government marking of CUI prior to the transmission of such CUI or clear instruction to the contractor when their performance under a contract will create defense-sensitive CUI.

Agency personnel generally default to overmarking information as CUI to minimize risk acceptance, which leads to emails, basic documents, presentations, and other communications being incorrectly marked as CUI. NDIA is aware of multiple situations where the lack of understanding of what should and should not be considered CUI and how the Department stores, handles, and transmits defense-sensitive CUI leads to confusion and potential security issues.

As an example, mypay.dfas.mil is utilized by military personnel and retirees. The current landing page is viewable to the public yet has "CONTROLLED UNCLASSIFIED INFORMATION" printed across the bottom of the page and across every page a valid user accesses from their home computers using their personal internet service providers. At the other end of the spectrum, presenters at public forums presented slides marked CUI that did appear to contain sensitive technical data. However, nothing prevented audience members from taking pictures of the slides and sharing them more broadly. While the proposed rule states that "CMMC does not in any way change the DoD requirements regarding the definition, marking, and protection of CUI," it is exactly those requirements driving the inconsistencies, ambiguities, and inaccuracies within the current process leading to confusion, increased costs, and decreased security for all parties.

If the specific CMMC rule cannot or will not address DoD requirements regarding CUI, then the CMMC and CUI stakeholders in the Department must tackle this challenge to effectively safeguard CUI and implement CMMC requirements. It is imperative that the government specify and clearly define CUI, complete the promulgation of associated contracting clause regulations that are almost seven years old, and, most importantly, for the success of this undertaking, impose and implement an effective and consistent document marking process for the DoD and all government agencies to utilize on a consistent basis. Without these actions, industry cannot effectively, consistently, and successfully protect CUI, making it impossible to reach the level of protection these standards and the corresponding contracting clauses seek to achieve.

NDIA would recommend engaging in a formalized process and working with industry and across the government to establish clear and consistent CUI identification and marking guidance to ensure the security of the data and information that needs to be protected. This will alleviate the unnecessary burdens and costs associated with protecting frivolous information and ensure the government and industry can focus resources on protecting the data and information that truly matters by determination.

CMMC 2.0 Increases the Cost and Scope of Compliance Beyond Current Contractual Requirements

The proposed rule does not include estimates of the costs associated with implementing the existing cybersecurity requirements under FAR clause 52.204–21 or associated with implementing NIST SP 800–171 requirements in accordance with DFARS clause 252.204–7012. Further, the proposed rule states that these costs should have already been incurred "[t]o the extent that defense contractors or subcontractors have already been awarded DoD contracts or subcontracts that include these clauses, and process, store, or transmit FCI or CUI in support of the performance of those contracts."

NDIA offers, however, that CMMC 2.0 does increase the scope and costs of the program beyond current contractual requirements. Cost is not simply determined by the number of security requirements in an underlying standard. Strictly speaking, the number of security requirements has not changed. The number of systems and organizations, however, outside of the principal organization to which these requirements apply has been increased, and that expansion of the scope of application does increase the cost significantly.

Other factors driving additional costs for vendors include the introduction of new terms. Security Protection Assets (already published in CMMC 2.0 documentation) and Security Protection Data (introduced in this rule) increase the scope of application of the requirements beyond what is listed in DFARS clause 252.204–7012 and, therefore, increase direct implementation and compliance costs above and beyond the admitted assessment costs.

These changes will increase costs for nearly all members of the DIB and are especially impactful for small and medium businesses and nontraditional defense contractors. It will also drive costs to "rip and replace" existing tools and will likely involve the purchase of more expensive FedRAMP or CMMC-certified tools, which all drive enhanced costs for security requirement implementation, not counting the additional assessment costs.

The recently released National Defense Industrial Strategy (NDIS) outlines the Department's goals to attract new entrants in addition to fostering long-standing DoD partners. NDIA would note that this inconsistency in requirements and strategy, coupled with a lack of understanding of the full costs associated with meeting the Department's cybersecurity requirements, can create and sustain barriers to start-ups, small businesses, and nontraditional suppliers and vendors to the industrial base. As such, it would be helpful for the DoD to include the costs associated with compliance with DFARS clause 252.204–7012 to understand the full cost of requirements associated with DoD partnerships.

Without question, this rule will increase the cost of serving government customers across the DoD, and the Department should squarely and transparently address this fact.

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

DoD Should Provide Clarity and Issue a Class Deviation to Afford Additional Time for the Transition from NIST SP 800-171 Revision 2 to Revision 3

As the Department is aware, the standards to update NIST SP 800-171 from Revision 2 to Revision 3 are expected to be finalized in early 2024, which includes the assessment documentation in 800-171A. Industry continues to invest in a conformance model based on Revision 2 of 171 and Revision 1 of 171A.

CMMC 2.0 is linked specifically to Revision 2, but the current requirement for covered defense contractors, as specified in the DFARS, is not linked to a specific NIST Revision. This disconnect represents a strategic issue overall for this proposed rule and creates more confusion for industry than it resolves. The DFARS clause reliant on these NIST standards specifies that compliance is based on the standard in force at the time of a solicitation as passed through a contract, which means an industry partner or vendor requires planning, resources, and budget for acquisition, implementation, and operation. Analysis of NIST's current final public draft estimates a 75 percent difference in security requirements and parameters to achieve compliance from Revision 2 and Revision 3. In addition, the DoD Supplier Performance Risk System (SPRS) would require significant upgrades to support the language and specification in both DFARS 252.204-7012/7020 and as prescribed in the DFARS Part 204.7304 solicitation provision and contract clauses.

Causing further confusion, the accreditation body for CMMC has publicly stated they will need at least a year after the finalization of the standard in order to revise all documentation, re-train and re-certify assessors, and re-accredit CMMC Third Party Assessment Organizations (C3PAOs) to the new standard in Revision 3. Finally, the CMMC regulations position industry to be reliant upon these misaligned standard revisions, accreditation and assessment updates, and regulatory effective dates, all of which create a substantial challenge for industry to understand and implement with Plan of Action and Milestone limitations in an effort to protect CUI.

NDIA strongly recommends and encourages the DoD CIO office to work with NIST and the FAR and DAR Councils to develop a phased approach of at least a year to transition from Revision 2 to Revision 3, currently and during the implemented CMMC phases. The Department should establish clear implementation dates and milestones indicating when industry should shift investments in cyber protections for data from previous iterations of the NIST SP 800-171 standards to the latest version while aligning with international standards.

NDIA would also recommend that the Department consider issuing a class deviation to allow contract holders to effectively maintain protections for data, while not being misaligned with compliance requirements. Without clearly delineating effective dates and having a phased implementation period, the government risks having to maintain, assess, and audit multiple varying standards that employ differing assessment tools and guidance across hundreds of thousands of industrial base partners solely based on data protection as systems and environments vary and operate globally. This misalignment can and should be addressed before the application of Revision 3 upon the CUI effort.

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

Narrow the Definition of "Cloud Security Provider" and Define Additional Terms

NDIA is encouraged that the proposed rule distinguishes between Cloud Service Providers (CSPs) and other types of External Service Providers (ESPs), such as Managed Service Providers (MSPs). CSPs and MSPs each play a functionally distinct role in the DIB cybersecurity ecosystem. Many (or most) small businesses in the DIB rely on MSPs for IT and security services, making MSPs a critical leverage point for the success of the CMMC program.

NDIA supports the requirement for MSPs to achieve CMMC certification at a level equal to or greater than their DIB clients, but we are concerned that the proposed rule does not sufficiently disambiguate CSPs from other types of ESPs, such as MSPs. This will lead to confusion, slowing down the CMMC rollout and increasing costs for Organizations Seeking Assessments (OSAs).

The proposed rule's definition of Cloud Service Provider is broad and diverges from well-understood definitions of cloud computing, such as those in NIST SP 800-145 and DFARS 252.239-7010.

This is problematic because, relying solely on the definition in § 170.4(b), an OSA or C3PAO may conclude that an MSP falls into the category of "an external company that provides... applications... for its clients" and must, therefore, meet the FedRAMP requirements for CSPs. This interpretation would be logical based on the text of the proposed rule but not in line with a common understanding of cloud services—that is, not all "provide[d]...applications" are Software-as-a-Service (SaaS) or constitute cloud services.

NDIA urges the DoD to adopt a narrower definition of Cloud Service Provider, derived from NIST SP 800-145, for clarity and consistency with other DoD regulations and alignment with other government-wide applications. One possibility is to reference the definitions of Cloud Service Provider and Managed Service Provider found in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA):

- **Cloud Service Provider**
  "The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document relating thereto."

- **Managed Service Provider**
  "The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center."

NDIA expects that most MSPs will not process, store, or transmit CUI, but are likely to handle Security Protection Data. The CMMC rule should also define the new term "Security Protection Data" in § 170.4(b).

Require a Customer Responsibility Matrix (CRM) From All ESPs

Just as CSPs are required to provide a Customer Responsibility Matrix (CRM), ESPs other than CSPs should be required to provide a document detailing how responsibilities for control implementation are shared between the service provider and the customer. Outside of the FedRAMP context, the industry-accepted term for such a document provided by an MSP is a "Shared Responsibility Matrix" (SRM).

The CMMC rule should mandate that ESPs other than CSPs provide an SRM. The rule should also specify how CRMs and SRMs should be assessed and/or validated during CMMC Self-Assessments and Certification Assessments. NDIA notes that the proposed rule creates a logical dependency where an OSA using an MSP cannot complete CMMC Level 2 or Level 3 scoping until the MSP receives a CMMC Final Certification Assessment. Therefore, it is imperative to clearly distinguish MSPs from CSPs and prioritize them in the assessment process to prevent delays in the CMMC rollout.

Increase Flexibility for the Use of Plans of Action and Milestones (POA&Ms) and Attestation

POA&Ms are an effective management tool that help organizations prioritize and manage cybersecurity risks effectively. NIST SP 800-171 addresses and recognizes the importance of POA&Ms where it states:

> "The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization."

NDIA appreciates the ability to utilize POA&Ms and the proposed contract-specific waiver within CMMC 2.0. We believe, however, that limitations are constraining and propose that increasing the flexibility and assessment of POA&Ms within the proposed rule will better align their essential risk management role with the realities faced together by industry and government today, as well as support future developments relating to zero trust, quantum computing, and artificial intelligence.

Close to two-thirds of the 320 assessment objectives in Level 2 are related to requirements that are not eligible for POA&Ms, and the remaining requirements have only a six-month grace period before also becoming ineligible for POA&Ms. At a minimum, the rule can be made more accommodating to industry, without introducing insecure providers, by simply making it clear that companies may have any number of failed objectives re-assessed for up to six months after the original assessment, without undergoing a new full assessment. The companies would only receive a CMMC certification if they can show that they have implemented all requirements (or are eligible for 180-day POA&M as described in the rule). Rather than force companies to undergo multiple onerous full-scope assessments as proposed by the rule, this simple change would encourage companies to resolve deficiencies quickly and enable them to be reassessed at a more affordable cost.

PO&AMs are a useful tool to facilitate compliance, and contractors should not be punished for utilizing them. In the world of cyber risk mitigation, it is impossible to maintain perfect implementation of an IT system on a continuous basis as change is constant. Government and industry need to constantly update, patch, and reconfigure systems as threats evolve. As outlined in the proposed rule, "If the CMMC PMO determines that the provisions of Level 1 of this rule have not been achieved **or maintained** [emphasis added], as addressed in § 170.6, a revocation of the validity status of the CMMC Level 1 Self-Assessment may occur. At that time, standard contractual remedies will apply and the OSA will be ineligible for additional awards." If a company acknowledges a control issue and agrees to mitigations under a POA&M, the company could face the risk of being assessed "standard contract remedies."

Additionally, the proposed rule requires affirmation of the OSC's compliance with security requirements: "the affirming official shall submit a CMMC affirmation attesting to continuing compliance with all CMMC Level 1 security requirements." A single patch or Federal Information Processing Standard (FIPS) validation status change, however, could result in thousands of companies being determined to be in violation of Federal Law and potentially subject to damages, penalties, law enforcement actions, and more under the False Claims Act. Companies should not face this liability because they took prompt action to maintain system security by installing the patch or FIPS update. This action could technically be deemed to render a control out of compliance even though the intended action was to continue to maintain security and compliance on a continuous basis via the standard NIST requirement for risk assessment and the use of POA&Ms to manage temporary deficiencies. The CMMC proposed limitation should be revised to provide appropriate treatment of such actions, supported by rational valuations of the combined risks, adjacent controls, and mitigations.

We note that there is a significant difference between the CMMC-AB guidance on how to handle these types of issues and the DCMA's own assessment guidelines. DCMA has indicated that they would rather an organization stay up to date on security patching in line with the vulnerability remediation controls than delay patching and have a security vulnerability merely to keep the FIPS control met.

For these and similar types of situations, NDIA would encourage the Department to allow organizations to utilize POA&Ms for areas of non-compliance beyond their control.

Reciprocity across Nations, Governments, Agencies, and Contracts

We encourage DoD to explicitly address in the CMMC rule how the CMMC program will handle issues of reciprocity, portability, and scalability of a CMMC certification across different governments (domestic and international), agencies, and contracts. For instance, recognizing and transferring CMMC certifications or self-assessments among the Five Eyes, other allies, or in Foreign Military Sales contracts.

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

Clarify Prime Contractor/Subcontractor Roles and Responsibilities; Flow Down Requirements

The proposed rule imposes a flow down of CMMC requirements from prime contractors to subcontractors in the supply chain. Prime contractors are also tasked with requiring subcontractor compliance throughout the supply chain at all tiers as per the applicable CMMC level for each subcontract depending on contractual obligations pursuant to § 170.23(a).

In some cases, the prime and subcontractor could be subject to different CMMC Levels. In other cases, they could have multiple contracts requiring different levels. The prime and subcontractor also could be in a position where their roles are reversed—such that the subcontractor could be the prime and the prime could be a subcontractor in another contract—and the subcontractor could, and may, be forced to evaluate the other's compliance on other contracts. A prime and subcontractor could have multiple contracts where this occurs.

It is already difficult for some subcontractors and suppliers to comply with and implement NIST SP 800-171 controls. Making prime contractors responsible for oversight and verification of compliance of their entire defense supply chain will place substantial risk and liability on prime contractors that have neither the resources nor the ability or insight to adequately manage and effectively oversee subcontractor CMMC compliance on such a large scale and on a continual basis. We strongly encourage the DoD to explicitly clarify the relationship, roles, and responsibilities between the prime and subcontractor under the CMMC rule.

The proposed rule also does not make clear how CUI level requirements will be determined—whether by program or by the sensitivity of data disclosed. If determined by the sensitivity of the data, will DoD create three new CUI category markings? If determined by the program, will sub-tier suppliers receiving less sensitive data still need to comply with the requirements based on the prime contract level? For example, will a small supplier receiving limited and less sensitive data to make nuts and bolts for a Level 3 prime contract be required to comply with Level 1 or Level 3? Who will make these decisions, and how? It is critical to clarify how CUI will be identified by "level" or by "categorization" to allow for appropriate flow down and protection and to simplify CUI by avoiding the creation of more categories of CUI under an already confusing and inconsistently applied CUI program. We reiterate our call for the Department to engage in a formalized process with industry to establish clear and consistent CUI identification and marking guidance that can also address the identified flow-down issues.

Application to Subcontractors

Although the flow-down requirements for first-tier subcontractors can be easier to enforce by prime contractors due to their direct contractual relationship, the same is not the case in a multi-tier scenario where the ability of the prime contractor to confirm and enforce CMMC requirements is limited. A lack of privity between prime contractors and lower-tier subcontractors and suppliers creates a barrier to collecting valuable information that will allow a prime to confirm that CUI is properly safeguarded.

A recommended solution for addressing a prime contractor's lack of information in multi-tier situations where CMMC flow downs have occurred is to allow the prime access to assessments and attestations contained in the Supplier Performance Risk System (SPRS) concerning any subcontractor performing within the supply chain of the prime's government contract. This information should also be accessible to any higher-tier subcontractor as a risk management tool. The result of more transparent SPRS data is that it would allow prime contractors to exercise more effective enforcement for compliance with CMMC safeguarding requirements.

The fact that prime contractors do not have access to supply chain SPRS data is one factor in a greater "information" problem that DoD should address. In order to ensure a competitive edge, prime contractors may create closed supply systems where they will force sub-tier suppliers to pursue certification far sooner than those subcontractors will actually need such a requirement in a contract. Because primes do not have accurate information about timing and compliance requirements for future contracts, they will believe their risk is exponentially increased if they do not pre-emptively "flow down" CMMC requirements and take responsibility for pushing same-level CMMC certification requirements. Prime contractors may push a higher requirement level on their supply chains, and in some cases, such as for Level 3 certification, these supply chains will needlessly burden CMMC certification efforts.

A recommended approach to this lack of information problem is for DoD to provide proper lead times on contracts. Also, disincentives for pushing needless requirements, such as not providing credit for superfluous levels of certification during award assessments, may dissuade primes from seeking to overburden their supply chains.

Finally, DoD should address the possibility that a bottleneck for certification could result, particularly in the early stages of CMMC implementation, where a prime, or one of its subcontractors, is not yet at a requisite CMMC level for a procurement but through no fault of their own. In such a scenario, a bidder could protest a solicitation because it or its subcontractor is being kept out of competition due to a slow CMMC process. While NDIA has not conducted an analysis of how different adjudicative jurisdictions may address this question, the DoD should avoid placing itself and the DIB in such a situation. Instead, the DoD should ensure that all contractors and subcontractors have the opportunity to bid on a contract. Only through proper planning, timing, and massive investment by DoD to ensure that sufficient assessment support is in place can an efficient and fair CMMC program be realized.

Further Clarification Request

A portion of NDIA companies processed through Joint Surveillance have been previously informed by the Department that successful completion, i.e., a perfect score, would result in a three-year CMMC certification from the time the rule went into effect. The current rule states the DIB member will be certified with a perfect score for three (3) years from the date of the audit. We request clarification whether it is the intent of the Department to base the three-year extension from the initial review or the date the final CMMC rule goes into effect.

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

Conclusion

NDIA and its membership appreciate the government's desire to promote a strong, dynamic, and robust defense industrial base. We do, however, have concerns surrounding certain aspects of this proposed rule. For the reasons raised in our comments, we respectively suggest changes considering the unique challenges faced by companies that operate in the defense sector. NDIA stands ready to assist in revising and updating these proposals and would welcome this collaboration.

NDIA appreciates the opportunity to provide comments on the proposed rule for CMMC 2.0. If you have any questions related to these comments, please reach out to Michael Seeds at mseeds@ndia.org.

Sincerely,

National Defense Industrial Association