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

October 15, 2024

Ms. Heather Kitchens
OUSD(A&S) DPC/DARS
3060 Defense Pentagon
Washington, DC 20301-3060

Electronic Submission: *www.regulations.gov*, DFARS Case 2019-D041

Re: Comments on the Proposed Rule for Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

Dear Ms. Kitchens:

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide comments on the proposed rule for assessing contractor implementation of cybersecurity requirements, DFARS Case 2019-D041, related to the Cybersecurity Maturity Model Certification (CMMC) Program.

NDIA is the nation's oldest and largest defense industry association, representing over 1,700 corporate and close to 65,500 individual members from small, medium, and large contractors, a majority of which are small businesses. NDIA members design, manufacture, apply, and maintain the cutting-edge technologies, systems, and platforms that our armed forces rely upon to deter aggression and defend our nation and its interests.

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. As such, our members' professional and informed views on this request for information reflect the complexity and nuance of the issues under discussion.

Our pacing competitor and near-peer competitors work every day to steal commercial and personal IP, financial, and health information and to undercut the U.S. military's competitive advantage on the battlefield. For these reasons, NDIA and our member companies long ago committed to the necessity of security for the data and systems that power the U.S. 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 offers the following comments and recommendations on the proposed rule:

72-Hour Reporting to Contracting Officer Efficacy

The proposed rule introduces a requirement to notify the contracting officer within 72 hours when there are any lapses in information security or changes in the status of the CMMC certificate or CMMC self-assessment levels during the performance of the contract. This new requirement introduces unnecessary steps that should be handled via the DIBNET Portal and Supplier Performance Rating System (SPRS) systems we use today.

When DIB companies experience a security incident, they are already required to report it within 72 hours via the DIBNET portal, which then notifies all affected contracts. This process helps streamline and make the reporting process more efficient. By requiring the DIB company to individually notify each contracting officer, this new process risks slowing down the pace at which notifications can be made and also consumes the DIB company's time and resources that could be spent managing the lapse/incident. Similarly, a company's compliance with DFARS cybersecurity is managed via the SPRS website, where government contracting officers can check and monitor for supplier compliance in a single location. The requirement to individually notify contracting officers about CMMC status will introduce extra work for little to no additional value, and SPRS has already solved this process.

The proposed rule introduces the term "lapse" in relation to cybersecurity and potential incidents. However, the rule does not clearly define what constitutes a "lapse," which again could lead to confusion and increased work activity from DIB companies. Even with a narrow definition, lapses in information security are too broad a reporting requirement. This is also another expansion of the overall requirements. Nearly anything could be construed as a lapse in information security. If someone holds the door open for a fellow employee in violation of policy requiring them to badge in, then that now becomes an offense reportable to the DoD. Any number of things that are daily parts of real operations are potentially lapses in information security. Every time an employee clicks the link, it is a lapse of information security, and these types of examples are nearly limitless. NDIA recommends that these requirements be removed and instead leverage the systems that DoD already has in place to maintain visibility of these areas.

Senior Official Attestation and Modification of System to Address Bug Fixes, Cybersecurity Incidents

The term "affirmation" has not been used in DoD contracts to date, but representations exist and are operational in federal contract administration and management by authoritative regulation. The rule introduces the requirement for an affirmation of continuous compliance with security requirements. However, it is unclear what is included in the affirmation and how it is to be measured. As previously submitted under 32 CFR 170, the affirmation of continuous compliance, where compliance is defined as the complete and perfect implementation of all 110 Controls/320 Assessment Objectives over time and indefinitely into the future, is not possible. An affirmation is the equivalent of a legal oath, and this regulation directs that contractor senior officials swear that they will always be compliant in the future under the threat of federal criminal fraud charges should they fail.

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.

NDIA would recommend removing the affirmation requirements altogether, as the CMMC program introduces third-party certifications that should serve to indicate the company's compliance. A continuous affirmation adds little value to the process while creating addition work and unnecessary legal risk.

Flowdown Requirements

Industry requests further clarification around the flowdown of CMMC requirements to subcontractors and the lack of a standardized mechanism for prime and subcontractors to verify the compliance of their subcontractors. 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.

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. NDIA strongly encourages the DoD to explicitly clarify the relationship, roles, and responsibilities between the prime and subcontractor under the CMMC rule.

DoD Supplier Performance Rating System (SPRS) and Compliance Responsibility

As proposed, the exclusion of paragraphs (b)(5) and (c) in subcontracts appears in direct conflict with how entries for contractors and subcontractors are managed in the DoD Supplier Performance Rating System (SPRS). These requirements should be harmonized.

It is also unclear whether the intent of the proposed clause exclusion is for only commercially available off-the-shelf (COTS) items or to require that prime companies manage proposed affirmations of

continuous compliance and certifications/attestations of compliance for subcontractors and suppliers independent of (and without the benefit of) SPRS DoD Unique identifiers (UIDs).

Prime contractors should not be required to prove the compliance of all subcontractors. 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. As we stated previously, the CMMC program introduces third-party certifications, which should serve to indicate the company's compliance.

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 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.

An alternative option would be to limit the scope of 252.204-7021(b)(6) to direct suppliers without requiring enforcement throughout the entire supply chain. This is similar to the approach taken in 252.204-7021(d) and would flow down the enforcement responsibility to the most appropriate contracting tier.

CUI vs. FCI

The rule states "(i) The results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract posted in the Supplier Performance Risk System (SPRS) (see 32 CFR 170.15 through 170.18); and.." This could be interpreted to mean that if a CMMC Level 2 certification is specified in a contract, all FCI information would be required to operate at Level 2, which is not a requirement for that information type as outlined in FAR and DFARS. We believe it is the DoD's intent to allow for multiple systems per contract, as they have estimated an average of five systems in this proposed regulation, and some of those systems might be FCI, i.e., Level 1 specific. NDIA recommends this language be adapted as follows:

> 204.7502. Policy. (a) The CMMC certificate or CMMC self-assessment level specified in the contract for specific is required for all information systems, used in the performance of the contract, that will process, store, or controlled unclassified information (CUI). Information systems processing Federal Contract Information (FCI) and not CUI require a CMMC Level 1 self-assessment.

> 204.7503. Procedures. (i) The results of a current CMMC certificate or current CMMC self-assessment at the level required by the solicitation, or higher, for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that will process, store, or transmit CUI and that will be used in performance of the contract posted in the Supplier Performance Risk System (SPRS) (see 32 CFR 170.15 through 170.18). Systems processing FCI and not CUI require a CMMC Level 1 self-assessment.

If the intent was to require all FCI handling to occur within the CUI-certified boundary, then this is largely inexecutable across the DIB and represents another significant expansion of requirements. NDIA recommends that the language be clarified to allow a contractor that only does some DoD work to continue to use their existing and compliant business systems for the processing of FCI and build an enclave at the higher security requirement level for CUI. This is both an important option to control cost and one that has been under construction broadly in the DIB based on existing guidance.

Discretion on CMMC inclusion in solicitations.

CMMC is proposing a phased approach to the implementation of CMMC requirements in contracts. However, it leaves those determinations up to the discretion of the program without transparent methodology on how they should decide. Allowing discretion at the program level with no clear methodology or control method risks CMMC requirements rolling out sooner and in greater volumes than the DIB and C3PAOs may be able to support. This will have the effect of essentially cutting several DIB companies out of competing for contracts and offering DoD best value, as well as potentially causing smaller businesses to exit the market because the contract requirements are increasing at an unsustainable rate. This could also impact the ability of high-priority contracts that have a strong need for CMMC certification to obtain qualified suppliers.

NDIA recommends the DoD publish the methodology by which programs determine the CMMC level and the timing of the certification requirement, this would ensure greater transparency and ability to negotiate with programs that might be overly aggressive in their desire to adopt CMMC and negatively impact DoD's ability to extract best value from the DIB.

Approval Process for CMMC Inclusion in Solicitations and Contracts is Missing

The text from the current DFARS 204.7503 Contract Clause dated Sept. 29, 2020, should be modified with phased dates and approvals from DoD CIO/CISO CMMC Program Management Office and/or OUSD(A&S) per the following inclusion and changes (strikethroughs and changes in red font). Use the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement, as follows:

(a) Until September 30, 2028, in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level 2 or 3 certificate. In order to implement a phased rollout of CMMC, inclusion of ~~a~~ the CMMC requirement in ~~a solicitation~~ FAR Part 16 Types of Contracts during this time period must be approved by OUSD(CISO) CMMC PMO and/or OUSD(A&S).

b) On or after October 1, 2028, in ~~all~~ FAR Part 16 Types of Contracts solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts or orders solely for the acquisition of COTS items.

Additional Clarification of Terms

NDIA respectfully asks for greater clarity on the following terms used in the rule and the activities required:

- The use of the term "data" in the CFR does not clearly state how it defines and applies this term, which will cause confusion and potentially impact systems in scope, as that term could be interpreted broadly. NDIA recommends that the government narrowly define the categories of data to which the rule applies (e.g., CUI or FCI).

- The rule introduces the term DoD unique Identifier, but it is unclear how these will be assigned, how they will be different from cage codes used today, and how they will link back to a company's cage codes. Risk introduces another layer of complexity and confusion with unclear benefits/goals. NDIA recommends either sticking to the Cage Code linkages in SPRS used today for tracking compliance to DFARS 252.204-7020 or at least clarifying how the DoD UI process will work and be used.

- The rule now uses the term "Contractor Information Systems" where previous guidance has used "Covered Contractor Information System", this again risk broadening the scope of applicability to system unrelated to CUI and FCI, such as COTS and SaaS. NDIA recommends the government narrowly define what the term "Contractor Information System" means or revert to the old term "Covered Contractor Information System."

Conclusion

NDIA and its membership appreciate the government's desire to promote a strong, dynamic, and robust small business industrial base. We do, however, have concerns surrounding certain aspects of

these proposed rules. 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. If you have any questions related to these comments, please reach out to Michael Seeds at mseeds@ndia.org.

Sincerely,

National Defense Industrial Association