ITI Promoting Innovation Worldwide

October 10, 2024

Sent via the Federal eRulemaking Portal: https://www.regulations.gov

Ms. Diane Knight Department of Defense
Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate
4800 Mark Center Drive
Suite 08D09, Alexandria, VA 22350–1700
E-mail: osd.mc-alex.dodcio.mbx.cmmc-32cfr-rulemaking@mail.mil

Public Comments from the Information Technology Industry Council on DFARS Case 2019-D041, Proposed Rule Affecting 48 CFR Parts 204, 212, 217, and 252.

The Information Technology Industry Council (ITI) appreciates the Department of Defense's (DoD) continued commitment to promoting the adoption of security practices across the Defense Industrial Base (DIB). ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

We appreciate the straightforward nature of this Rule. It reflects the hard work that the Department and the DIB have put in over the course of the last few years. In our view, the Rule a) is consistent with DoD's communications around the CMMC program; b) appropriately exempts commercial off-the-shelf (COTS) products; and c) adheres to an appropriate phase in period.

Below, we make seven recommendations that we believe will further strengthen the implementation of the Rule. Specifically, we recommend that the Department: 1) Broaden 202.7502 (c) to avoid duplications with comparable Federal assessments rather than limiting this policy to comparable DoD assessments only; 2) Harmonize incident reporting requirement with existing federal requirements; 3) Amend Section 204.7501 to outline permissibility of conditional certifications; 4) Provide additional guidance on how future updates to the underlying NIST standards will be addressed in regulatory implementation

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

and contractor compliance; 5) Create formal waiver procedures that procurement officials can grant; 6) Provide generalized visibility into subcontractors' certification status; and 7) Clarify at what point subcontractors must be compliant.

Broaden 202.7502 (c) to avoid duplications with comparable Federal assessments rather than limiting this policy to comparable DoD assessments only

We welcome the acknowledgement that this rule does not exist in a vacuum and explicitly support the intent behind the statement in Section VI that reads "This proposed rule does not duplicate, overlap, or conflict with any other Federal rules." It is in this spirit of ensuring regulatory alignment and harmonization that we recommend that Section 202.7502 (c) of the Rule's policy language be adjusted to read "The CMMC assessments shall not duplicate efforts from any other comparable ***federal*** assessment, […]" [emphasis added]. This modification would streamline the assessment process for Organizations Seeking Certification (OSCs) and directly support the objectives outlined in the DoD Cybersecurity Reciprocity Playbook[1] that discusses the benefits and conditions for cybersecurity reciprocity. Additionally, we also recommend the Department continue its outreach to global partners and allies to promote international harmonization and mutual recognition of required assessments and regulations.

Harmonize incident reporting requirement with existing federal requirements

We have concerns with the new 72-hour reporting requirement in the proposed clause at 252.204-7021 (b)(4) stating: "Notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract". Introducing an additional incident reporting requirement contradicts the federal harmonization efforts on cyber incident reporting.[2] Moreover, it duplicates the existing reporting requirements under 252.204-7012.

Specifically, the reporting requirement is problematic in at least 3 aspects:

1. It remains unclear what "any lapses in information security" means, particularly given the broad definition of "information security" at FAR 2.101. The final rule should clearly differentiate between "lapses" and "cyber incident", and the terms should be used consistently across all government guidance and regulations (e.g., CIRCIA, DC3 DIBnet -7012 reporting mandate, etc.).

[1] https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf

[2] In 2023, the Cyber Incident Reporting Council published a report entitled Harmonization of Cyber Incident Reporting to the Federal Government, available at: https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf

2. The current language implies that the 72-hour reporting window would start at the time of the lapse, not at the time of discovery, and
3. The reporting requirement to the Contracting Officer is impractical for lower-tier suppliers.

This reporting requirement is much broader, more ambiguous, and more burdensome than the current reporting requirement under 252.204-7012, which will also apply to contracts/subcontracts when the -7021 clause applies. The existing clause at 252.204-7012 already addresses the 3 problematic aspects in the following ways:

1. It defines more clearly what events need to be reported by defining "cyber incident" as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein," and further narrowing reporting to only those cyber incidents that "affect a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract";
2. it clearly states that the 72-hour clock begins upon discovery of the cyber incident by defining "rapidly report" as meaning "within 72 hours of discovery of any cyber incident"; and
3. it requires reporting only to dibnet.dod.mil rather than to each contracting officer.

We strongly recommend focusing the incident reporting requirements pursuant to 252.204-7021(b)(4) solely on reporting changes in the status of the CMMC certificate levels or CMMC self-assessment levels during performance of the contract. In our view, the 72-hour reporting requirement at 252.204-7012(c) provides sufficient notification of relevant information security incidents.

If there is a risk-based need to centrally collect and manage lapses in information security at a more granular level, we believe DoD needs to precisely define what constitutes a covered lapse. The final rule should clearly specify the types of “lapses” that would require reporting rather than using overly broad language. Moreover, the final rule should limit the reporting obligation to covered information systems containing controlled unclassified information (CUI) or federal contracting information (FCI).

The current, non-existent definition is overly broad and would inundate contracting officers with unactionable reports of possibly already mitigated lapses. We recommend that DoD identify an appropriate significance threshold that aligns with existing Departmental or federal reporting requirements. Moreover, if it is absolutely necessary to collect this kind of information for DoD risk management, those reports should be

collected through automated means, not by the Contracting Officer. To avoid duplication in reporting, we recommend amending -7012(c) to require contractors to report clearly and appropriately defined covered lapses through clearly defined, automated channels in addition to existing reporting requirements, rather than establishing an entirely separate set of reporting criteria under -7021. The government should aim for consistency for all reporting obligations across all government guidance and regulation (e.g., CIRCIA, DC3 DIBNet -7012 reporting mandate, etc.)

Amend Section 204.7501 to outline permissibility of conditional certifications

Per 32 CFR § 170.21, plans of actions and milestones (POA&Ms) are permissible if certain conditions are met. The presence of a POA&M may result in a conditional certification for up to 180 days from the initial assessment. Contracting officers cannot make awards, exercise contract options, or extend periods of performance unless contractors have an active certification and attestation of continuous compliance with CMMC in the Supplier Performance Risk System (SPRS) database, at the appropriate CMMC Level. In its current form, however, the Rule makes no mention of conditional certifications as a viable option for (sub-)contract award. We recommend amending Section 204.7501 Definitions to clarify that conditional certifications are acceptable for (sub-)contract award if the conditions in 32 CFR § 170.21 are met.

Provide additional guidance on how future updates to the underlying NIST standards will be addressed in regulatory implementation and contractor compliance

We appreciate and support the National Institute of Standards and Technology's (NIST) continued efforts to evolve standards in response to changes in technology, risk management, and security best practices. We also note that the proposed rulemaking lacks guidance or process on how future updates to the underlying NIST standards will be addressed in regulatory implementation and contractor compliance. We strongly recommend that the current class deviation for use of SP 800-171 Rev. 2 remains in effect while CMMC is in "phased rollout." DoD needs to develop a path forward with other Federal entities requiring NIST 800-171 to request, and accept, equivalency of CMMC Assessment certifications as sufficient and use a common baseline of organization-defined parameters (ODPs). A lack of equivalency will delay delivery of goods and services and increase cost of assessments if separate requirements are levied, and every Supplier will need to be assessed to different requirements.

Create formal waiver procedures that procurement officials can grant.

DoD-2023-OS-0063 (the 32 CFR Rule) states that during the phased implementation "DoD may elect to waive application of CMMC third party assessment requirements to a particular procurement." This Rule, however, is silent on whether waivers would be applicable and under what circumstances. During CMMC's three-year phase-in period, DFARS provisions may be added to some contracts but be absent in others. DoD waiver

authority could help prevent the halting or slowing of contract performance during the phase-in period at a minimal risk to DoD and other CMMC stakeholders.

It is unclear who has the authority to lower the requirement for a Tier 1 supplier to Level 1 if the Prime determines that there is no CUI passed to the Tier 1. Can lower levels of the Supply Chain make a self-determination of compliance with CMMC requirements based on the type of information flowed down in performance of the contract? If so, how will that determination be provided back up to the Prime and the contracting officer? Does the Contracting Officer need to be notified if the Prime decides to lower the Supplier to Tier 1? We recommend that DoD clarify the waiver authority by providing additional guidance on applicability for these common scenarios and by establishing a mechanism to submit questions as new ones arise.

Provide generalized visibility into subcontractors' certification status

252.204-7021(b)(6) requires contractors to ensure all subcontractors and suppliers complete and maintain an affirmation of continuous compliance with the security requirements with the required CMMC Level. This requirement extends to all tiers of the supply chain. *Part B. Analysis of Public Comments in Response to the Interim Rule Question 14* clarifies that contractors are expected to work with their suppliers to conduct verifications and *Question 29* reiterates that "contractors will only be able to access their own CMMC certificate and self-assessment information." We recognize and agree with the need to protect sensitive information. At the same time, we note that a manual, bilateral validation process will be cumbersome and may lead to oversights during the enforcement of 7021(b)(6).

Reaffirming or clarifying the terms of a contract is customary in contract administration and management in accordance with FAR 2.101 governing the acquisition and federal contracting process. We recommend that the final rule provide additional clarity regarding how contractors should navigate these requirements. We see at least two possible solutions that could improve this process. The first is to create an automated tool that provides upper tier suppliers with visibility into certification status without revealing supporting artifacts. The second 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.

Clarify at what point subcontractors must be compliant

204.7502(b) specifies that "contractors are required to achieve, at time of award, a CMMC certificate or CMMC self-assessment at the level specified in the solicitation, or higher." In our view, this will require the Prime and all tiers of the Supply Chain at "time of award" to be compliant with the Level issued under 252.204-7YYY even if the lower Tiers of the Supply Chain will not receive CUI as it is deconstructed down the Supply

Chain. This requirement will likely prompt contractors to default to requesting a Level 2 certification at all tiers, because there is insufficient information at time of contract award to make a reasonable assessment of the CUI flow down requirements. As a result, there will be additional delays in getting Suppliers on contract, reduced competition due to lack of qualified vendors, and increased cost to the government.

We recommend the final rule clarify at what point subcontractors must be compliant. The final rule should allow for enough time for primes to conduct subcontractor due diligence and require the Prime contractor to ensure that its sub-contractors should have the appropriate CMMC level ***prior to awarding*** a sub-contract or other contractual instrument. This should go hand in hand with defining a clear process to establish the appropriate CMMC level at lower levels of the Supply Chain based on the type of information that is being flowed down to the supplier. This ability to "decompose" the CMMC level required down the supply chain will be essential to successful implementation of CMMC and minimizing undue and unnecessary burden caused by blanket classification at Level 2 at Contract award.

We thank you for your consideration of our recommendations. If you have any follow up questions, please reach out to Leopold Wildenauer, ITI's Senior Manager of Public Sector Policy, at lwildenauer@itic.org.

Kind regards,

Gordon Bitko
Executive Vice President of Policy, Public Sector
Information Technology Industry Council (ITI)