Via email: www.regulations.gov

October 15, 2024

Leslie A. Beavers
Acting Chief Information Officer
Office of the Chief Information Officer
Department of Defense
Washington, DC 20301

Re: Proposed rule, Defense Acquisition Regulations System (DFARS), Department of Defense (DoD), Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041); Docket No. DARS-2020-0034; 89 *Federal Register*, August 15, 2024

Dear Ms. Beavers:

Our associations welcome the opportunity to comment on DoD's proposal to amend the DFARS to incorporate contractual requirements regarding the proposed Cybersecurity Maturity Model Certification (CMMC) 2.0 Program rule.[1]

We support the goals of the CMMC Program but have a number of overarching concerns for DoD and industry, including heightened costs, duplicative rules, and negative impacts on business innovation.

First, we want contractors to meet their cybersecurity requirements—particularly to enhance contractor resilience—but DoD culture plays a central role in performance outcomes. DoD's historical emphasis on cost, schedule, and performance is a main driver for its actions as well as the defense industrial base, or DIB. Increasingly, DoD leadership recognizes that the department's acquisition structure rewards cost, schedule, and performance more than integrated risk management capabilities, such as contractor cybersecurity.[2]

CMMC Program costs will depend upon several factors, such as a contractor's CMMC level, the complexity of a contractor's information system, and other market forces. Nonetheless, it is often overlooked that defense contractors are battling nation states and their proxies, which are amply resourced to target Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) for theft and misuse.

---

[1] https://www.federalregister.gov/d/2024-18110

DoD proposed rule, Cybersecurity Maturity Model Certification (CMMC) Program, *Federal Register* (*FR*), pp. 89058–89138, December 26, 2023. DoD proposes to add 32 CFR part 170 to the Code of Federal Regulations.
https://www.federalregister.gov/d/2023-27280

[2] *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, MITRE, August 2018, pp. 10, 19.
https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security

Our associations urge the administration and DoD to work closely with Congress to properly fund the CMMC. We want contractors to meet their CMMC Program requirements and receive fair compensation. By achieving this goal, the U.S. should improve its defenses against adversaries' operations against the DIB and impose costs on these actors and their malicious activities.

Second, DoD should avoid developing regulations that are sound in principle but sclerotic in implementation. For several years, policymakers have sought to better align, leverage, and deconflict policies, laws, and regulations to increase U.S. cybersecurity through improved efficiencies. However, progress is still largely aspirational. Depending on the products or types of services that contractors offer, they are likely subject to multiple assessments, certifications, and requirements across the federal government. Cloud service providers, for example, are required to meet many conditions in DoD's Cloud Computing Security Requirements Guide[3] and the Federal Risk Authorization and Management Program (FedRAMP).

DoD needs to put greater emphasis on helping policymakers and industry streamline existing cyber-related regulations (e.g., notifications and enterprise risk management mandates) to meet the CMMC Program in ways that bolster security and are cost-effective.[4]

Third, the House Armed Services Committee (HASC) held a hearing in September 2024 to examine why DOD struggles with rapidly developing and delivering innovation to U.S. warfighters. Lawmakers noted that the committee has led multiple efforts over the past decade to (1) enable DoD to create more flexible acquisition pathways and (2) partner with industry to expedite the fielding of innovative solutions to the military.

The hearing indicated that there is no shortage of innovative American businesses. Indeed, lawmakers called on DoD to better leverage, deploy, and scale our innovative advantages globally.[5] We favor strong cybersecurity standards, not onerous regulations. The CMMC Program should not be implemented unchecked, harming contractors' ability to innovate. Contractors and the department can agree that only sound cybersecurity practices, not rigid compliance, can best deliver cybersecurity to DoD stakeholders.

---

[3] https://public.cyber.mil/dccs

[4] A private entity told our associations that "myriad government contract clauses, guidelines, and rules make it imperative that the government works with business to harmonize federal cybersecurity requirements. Otherwise, the thickening red tape is going to (1) drive up contractors' costs without a corresponding increase in security, (2) hinder the timely completion of work for DoD, and (3) draw parties into endless battles over vague language and/or the meaning of regulatory provisions that should have been clear from the start. DoD can avoid such pitfalls by working closely with industry to drive CMMC Program clarity and alignment with similar federal requirements."

[5] HASC, "House Armed Services Committee Holds Hearing on Department of Defense Acquisition," *CQ Transcripts*, September 16, 2024.
https://plus.cq.com/alertmatch/656123348?0&deliveryId=135899669&uid=congressionaltranscripts-8085776&utm_medium=alertemail&utm_source=alert&openinplus=true

Our associations offer input on important themes and specific issues that have been underscored by several business groups, and we invite follow-up discussions with the department. Worth stressing, DoD should coordinate with Congress, agencies, and industry to push increased coherence to the proliferation of federal supply chain risk management initiatives that are underway.

Our comments are organized into the following 12 sections:

1. Reconsider including the 72-hour notification mandate, which is problematic and not harmonized with other cybersecurity reporting regimes.

2. Add the approval process for the inclusion of CMMC requirements in solicitations and contracts to the rule.

3. Clarify the term "data" and the scoping of the December 2023 and August 2024 proposals to reduce uncertainty and unnecessary costs.

4. Establish waivers, especially to enable contract performance during the phase-in period.

5. Develop guidance on flow-down expectations regarding subcontractors.

6. Allow contractors to verify subcontractor compliance in the Supplier Performance Risk System (SPRS).

7. Mitigate DIB compliance costs by streamlining CMMC requirements across DoD.

8. Push for harmonization and reciprocity between CMMC and other cyber certification programs.

9. Maintain the scope of safeguarded CDI and FCI under the CMMC Program.

10. Ensure that an information system processing FCI only needs CMMC Level 1.

11. Permit contractors to define the scope of an information system applicable to the DoD unique identifiers (UIDs) requirements.

12. Absent a safe harbor, eliminate affirmations of compliance by a senior company official from the rulemaking.

***

1. Reconsider including the 72-hour notification mandate, which is problematic and not harmonized with other cybersecurity reporting regimes.

The terms "any lapses in information security" and "changes" in CMMC compliance are problematic and undefined. The proposed language in DFARS 252.204-7021(b)(4) would require a contractor to report within 72 hours when there are "any lapses in information security" or "changes in the status of CMMC certification or CMMC self-assessment levels" during performance of the contract.[6] Our associations have significant concerns with this requirement, which is overly broad and ambiguous.

The wording "any lapses in information security" is not defined. It is unclear, for example, whether a notification would be required when a contractor's network is negatively impacted or slightly degraded compared to suffering a full-blown outage. It is also unclear whether human error in loading FCI or CUI into an environment outside of a CMMC enclave would trigger a notification.

According to Merriam-Webster, a lapse refers to "a slight error typically due to forgetfulness or inattention" or "a temporary deviation or fall especially from a higher to a lower state."[7] In addition, Dictionary.com defines a lapse as "an accidental or temporary decline or deviation from an expected or accepted condition or state; a temporary falling or slipping from a previous standard" or "a slip or error, often of a trivial sort; failure."[8] Put simply, a lapse is not significant.

Also, there is a lack of clarity about what constitutes "changes in the status" of a contractor's CMMC compliance under the 72-hour notification requirement. A contractor must attest to its "current"[9] CMMC self-assessment or certification, including "with no changes in CMMC compliance since the date of the assessment."[10] Current is defined, but changes is not.[11] DoD should consider specifying when changes would invalidate a self-assessment or

---

[6] *FR*, p. 66338.

[7] https://www.merriam-webster.com/dictionary/lapse
https://www.dictionary.com/browse/lapse

[8] A business told our associations that "a lapse should not be a reportable requirement; nor should it rise to a level of scrutiny so that the government could 'go after' a contractor's compliance posture."

[9] *FR*, pp. 66336.

[10] Ibid.

[11] *FR*, 66329.

A company told our associations, "DoD should address the ambiguity around 'security changes' in the proposed rule that may require additional attestation related to continued CMMC compliance. Similar to the ambiguity seen in the 'lapses in information security' language, it is unclear what would constitute the 'security changes' that DoD is referencing, including why they would need to be reported, particularly if they are not significantly impactful to a contractor's compliance or ability to maintain the appropriate certification level. We think that the requirement to report lapses in CMMC compliance should adequately cover DoD's concerns and that there should be no requirement to report security changes that are not significantly impactful to continuous compliance."

certification and when changes would be acceptable, thus not invalidating a contractor's compliance with CMMC.

The wording related to "lapses" in security and "changes" in the proposal is ambiguous regarding what circumstances would require reporting. For instance, one or both of the phrases could be interpreted to require the reporting of various types of security incidents that already require reporting under similar cyber incident reporting requirements applicable to contractors (e.g., FedRAMP and DFARS 252.204-7012).[12] The phrases imply that almost any circumstance that could be deemed to be noncompliant with the CMMC requirements, regardless of its significant, would require reporting. Such a requirement would result in the reporting of insignificant events and a diversion of resources to be compliant. Industry believes in the importance of reporting significant cyber incidents but not when there is little no benefit in reporting relative to its costs.

In addition, the notification requirement overlaps with cyber incident reporting requirements, such as DFARS 252.204-7012. DoD should clarify that the proposed language in DFARS 252.204-7021(b)(4) applies only to an information system that a contractor uses to process, store, or transmit FCI/CUI during the performance of the contract and is entered in SPRS.

Under DoD's proposal, the wording "any lapses in information security" could extend CMMC requirements far beyond protecting FCI/CUI. Per the proposed rule, the wording "any lapses in information security" would not be limited to FCI/CUI and could capture any change in a contractor's cybersecurity, which is impractical and not risk based. This wording could be interpreted to include elements of a contractor's network or information systems, not just those handling FCI/CUI. Contractors are developing discrete and often enclaved environments to be compliant with the CMMC Program. The focus of any notification requirements should be limited to CMMC-purposed information systems. To expect contractors—ranging from small startups to large multinational companies—to report lapses that have nothing to do with FCI/CUI is unreasonable, much less workable in practice.

Notifications are likely to be excessive, flooding a contracting (CO) with insignificant data and misusing contractors' time and resources. Under the proposed rule, a contractor must continuously comply with the security requirements associated with the CMMC level that is designated by a contract. Otherwise, it is supposed to notify a CO when changes occur (1) in CMMC compliance status[13] and (2) to the list of DoD UIDs applicable to each of the

---

[12] *FedRAMP® Incident Communications Procedures*, version 5.0, September 12, 2024. https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf

Under DFARS 252.204-7012, contractors must "rapidly report cyber incidents to DoD at https://dibnet.dod.mil." Rapidly report is defined as "within 72 hours of discovery of any cyber incident." https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

[13] *FR*, p. 66338.

contractor information systems that process, store, or transmit FCI/CUI and that are used in performance of the contract."[14]

According to the rulemaking, notifications must be submitted to a CO. It is far from clear what positives would come from notifying a CO, who may or may not be trained in handling and repurposing the data. Notifications, unless set at a high and risk-based level, would rapidly lead to excessive reporting by contractors and confusion for government officials. Such widespread notifications would be incredibly unproductive for nearly every party involved. Not only would notifications be burdensome to contractors, but alerts about temporary deviations in a contractor's compliance status would have little to no relevance in actually safeguarding FCI/CUI. COs would be overwhelmed with a flood of data that basically dilutes reporting that is objectively significant.

Instead of automatically notifying COs, contractors should have the option to report to DIBNet, which is DoD's network for online incident reporting and access to the DIB Collaborative Information Sharing Environment, or DCISE.[15] Ultimately, DoD and industry should collaborate to define the significant situations that would trigger notifications. This work should produce implementation guidance for contractors that is easy to use; it is also better aligned with the objective to protect government information and ensure cyber incidents that impact the government are shared with those who are capable of responding and investigating the source of the threat.

The proposed language in DFARS 252.204-7021(b)(4) stipulates that a contractor must notify a CO. Our associations understand how such notifications would work for a contractor. However, a subcontractor generally would not have privity of contract with a DoD customer, including not knowing who the CO is or how to directly contact the official. DoD should clarify that a subcontractor must notify the next higher-tier contractor (i.e., about any lapses in information security or changes in the status of its CMMC compliance), that would continue reporting up the chain of command. Finally, a contractor would notify the CO.

The notification mandate is not harmonized with similar cyber incident reporting regimes, which is detrimental to contractors' security. Our associations are concerned that the 72-hour notification requirement is not harmonized with related agency requirements, especially the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). While the proposed rule shares CIRCIA's 72-hour time frame for reporting to the government, the similarities end there.

---

[14] Ibid.

[15] https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE

DoD final rule on the voluntary DIB Cybersecurity Program, *FR*, March 12, 2024. https://www.federalregister.gov/documents/2024/03/12/2024-04752/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities

In sum, our associations urge DoD to strike the 72-hour notification requirement from the rulemaking unless the department can accommodate the following adjustments:

- Narrowly defining the terms "any lapses in information security" and "changes" in CMMC compliance and ensure that the definitions are tied to a contractor's information system.

- Consolidating the "lapses" and "changes" notification requirements into a single requirement rather than two.

- Aligning contractor notifications with the forthcoming CIRCIA rule, albeit amended (see Appendix).[16–17]

- Revising the thresholds for notifying DoD, which are too low and need to be amended to prevent overreporting by contractors and overwhelming COs with an unusable mass of data. Notifications should be pegged to *significant* lapses in information security and *significant* changes in a contractor's compliance posture (see the suggested bolded blue text below).

(4) Notify the Contracting Officer within 72 hours when there are any **significant lapses in information security for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract ~~or~~ and significant** changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract;

(5) Complete and maintain on an annual basis, or when **significant** changes occur in CMMC compliance status (see 32 CFR part 170), an affirmation of continuous compliance with the security requirements associated with the CMMC level required in paragraph (b)(1) of this clause in the Supplier Performance Risk System (SPRS) (https://piee.eb.mil) for each DoD unique identifier (DoD UID) applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and

(6) Ensure all subcontractors and suppliers complete and maintain on an annual basis, or when **significant** changes occur in CMMC compliance status (see 32 CFR part 170), an affirmation of continuous compliance with the security requirements associated with the CMMC level required for the

[16] A firm told our associations, "Owing to the numerous cybersecurity- and privacy-related reporting regimes that industry is increasingly subject to under state, federal, and international jurisdictions, the need to streamline notification obligations cannot be emphasized strongly enough."

[17] Worth flagging for DoD's attention, the Coast Guard is developing an approach for the maritime sector to report cyber incidents that is similar to CIRCIA's. The Coast Guard is on the correct path when it notes in its February 2024 rulemaking that harmonization "could allow more efficient use of DHS' cybersecurity resources and may advance the cybersecurity vision laid out by Congress in [CIRCIA]. . . . Information submitted to CISA would be shared with the Coast Guard, ensuring continued efficient responses."

What is more, the Coast Guard seems to suggest that its approach would facilitate the reporting of substantially similar information within a substantially similar time frame compared to CISA's proposed rule. Thus, a covered entity would likely be "excused from any duplicative reporting obligations under the CIRCIA rulemaking." The U.S. Chamber's May 2024 comments on the Coast Guard's proposed rule are available at https://www.regulations.gov/comment/USCG-2022-0802-0074.

subcontract or other contractual instrument for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

2. Add the approval process for the inclusion of CMMC requirements in solicitations and contracts to the rule.

The text from the current DFARS 204.7503 contract clause dated September 29, 2020, should be included and modified with phased dates and approvals from DoD's chief information officer, the CMMC Program Management Office and/or the Office of the Under Secretary of Defense for Acquisition and Sustainment, or OUSD(A&S), per the following recommended changes (see the strikethroughs and bolded blue text below).

Use the clause at 252.204-7021,[18] 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, 202**8**, 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.

Parent topic: Subpart 204.75—CYBERSECURITY MATURITY MODEL CERTIFICATION[19]

3. Clarify the term "data" and the scoping of the December 2023 and August 2024 proposals to reduce uncertainty and unnecessary costs.

According to the proposed rule, "data" must be processed, stored, or transmitted only on "information systems that have a CMMC certificate or CMMC self-assessment at the CMMC level required by the contract or higher."[20] The proposed rule does not define "data." Many in industry believe that data could be interpreted by DoD much more broadly than FCI/CUI. An

[18] https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements.#DFARS_252.204-7021

[19] DFARS 204.7503 Contract clause. https://www.acquisition.gov/dfars/204.7503-contract-clause

[20] *FR*, p. 66338.

elastic interpretation of data could effectively dissuade or prohibit contractors from handling or transmitting almost any kind of data with non-DoD agencies, outside attorneys and consultants, and subcontractors—to name a few—for fear of unintentionally running afoul of CMMC requirements.

In addition, the scope of the August 15, 2024, proposed rule covers "information systems that process, store, or transmit FCI or CUI during contract performance when a CMMC level is included in the solicitation."[21] In contrast, the scope of DoD's December 26, 2023, proposed rule applies to "any information system associated with the contract efforts that process, store, or transmit FCI or CUI, and to any information system that provides security protections for such systems; or information systems not logically or physically isolated from all such systems."[22] There is an obvious difference in the scoping of the two proposals, which would likely prove to be significant in terms of the regulated information systems and the costs to contractors. DoD is urged to resolve these differences by selecting a single scope for covered information systems.

4. Establish waivers, especially to enable contract performance during the phase-in period.

The proposed rule is silent on whether waivers would be applicable and under what circumstances. During CMMC's three-year phase-in period, a number of contractors' suppliers could receive a small amount of minimally sensitive FCI/CUI while coming into compliance. DoD waiver authority could help prevent the halting or slowing of contract performance during this trial period at a minimal risk to DoD and other CMMC stakeholders.

5. Develop guidance on flow-down expectations regarding subcontractors.

During the phase-in period, CMMC certification requirements must be flowed down to subcontractors at all tiers when a subcontractor processes, stores, or transmits FCI/CUI based on the sensitivity of the unclassified information flowed down to each subcontractor. Many contractors need guidance on DoD's expectations for flowing CMMC certification requirements to their subcontractors. For example, the proposed requirement for a contractor to flow down the CMMC requirements to a subcontractor in DFARS 252.204-7021(d) assumes a level of certainty about the information being flowed to a subcontractor. However, the reality is that most contractors flow down requirements based on what *could* occur at the subcontractor level. This precautionary thinking could be especially tempting in the context of CUI.

Further, imagine a scenario where a subcontractor's scope of work or the nature of its commercial product or service does not contemplate needing or generating CUI. But a contractor may determine that because it *could* or may need to share CUI with a subcontractor, the subcontractor must therefore certify or self-assess at CMMC Level 2. Under this scenario, the contractor may prefer to shift the burden of risk that its own employees may unnecessarily share CUI with the subcontractor by unnecessarily insisting that the subcontractor obtain a CMMC Level 2 certification or self-assessment, which could be quite costly, among other challenges.

---

[21] *FR*, p. 66328.

[22] *FR*, p. 89068.

Our associations recommend that DoD clarify the rule to say that if there is not an anticipated need for flowing down CUI to a subcontractor in the performance of a given contract, then such a subcontractor should not need a CMMC Level 2 certification or self-assessment to perform work on that contract. Also, the department should consider creating a mechanism for subcontractors to have unnecessarily high CMMC certification or self-assessment levels appealed or reviewed by an independent body of CMMC experts.

6. Allow contractors to verify subcontractor compliance in the Supplier Performance Risk System (SPRS).

According to the proposed rule, COs may not make awards, exercise options, or extend periods of performance under CMMC unless contractors and subcontractors have an active certification and an attestation of continuous compliance with CMMC requirements posted in the SPRS database.[23] However, DoD is not permitting a contractor to check its subcontractors' certification levels or attestations of compliance via SPRS even though DFARS 252.204-7012 requires contractors to (1) flow down all the requirements to their subcontractors and (2) confirm that their subcontractors have SPRS scores on file before DoD awards contracts.[24]

A contractor is responsible for its subcontractors but lacks a mechanism to independently validate a subcontractor's compliance with the CMMC Program. While attestations and certifications are standard industry practice for vetting third parties, the proposed rule assumes that contractors are ultimately liable for the noncompliance of their subcontractors. Contractors have limited control or visibility over subcontractors.

Our associations believe that a contractor should be able to confirm a subcontractor's attestations and certifications in SPRS. Contractors essentially want to verify that subcontractors have a valid driver's license and proof of insurance. Alternatively, DoD's rulemaking should include language explicitly permitting contractors to rely on the representations of subcontractors in SPRS similar to the Federal Acquisition Regulations (FAR) clauses 52.219-8 and -9 pertaining to small businesses, as captured below. Further, a contractor should not be held liable for any misrepresentations made by a subcontractor.

> **52.219-8 Utilization of Small Business Concerns. . . .**
> (e) (1) The Contractor **may accept a subcontractor's written representations** of its size and socioeconomic status as a small business, small disadvantaged business, veteran-owned small business, service-disabled veteran-owned small business, or a women-owned small business if the subcontractor represents that the size and socioeconomic status representations with its offer are **current, accurate, and complete as of the date of the offer** for the subcontract.[25]

[23] *FR*, p. 66338.

[24] *FR*, p. 89059.

[25] https://www.acquisition.gov/far/52.219-8
https://www.acquisition.gov/far/52.219-8#FAR_52_219_8__d3280e152

52.219-9 Small Business Subcontracting Plan. . . .

(2) (i) The Contractor **may accept a subcontractor's written representations** of its size and socioeconomic status as a small business, small disadvantaged business, veteran-owned small business, service-disabled veteran-owned small business, or a women-owned small business if the subcontractor represents that the size and socioeconomic status representations with its offer are current, accurate, and complete as of the date of the offer for the subcontract.

(ii) The Contractor **may accept a subcontractor's representations** of its size and socioeconomic status as a small business, small disadvantaged business, veteran-owned small business, service-disabled veteran-owned small business, or a women-owned small business in the System for Award Management (SAM) if–

(A) The subcontractor is **registered in SAM**; and

(B) The subcontractor represents that the size and socioeconomic status representations made in SAM are **current, accurate and complete as of the date of the offer** for the subcontract.

(iii) The Contractor may not require the use of SAM for the purposes of representing size or socioeconomic status in connection with a subcontract.

(iv) In accordance with 13 CFR 121.411, 126.900, 127.700, and 128.600, **a contractor acting in good faith is not liable for misrepresentations made by its subcontractors** regarding the subcontractor's size or socioeconomic status. [Emphasis added.][26]

7. Mitigate DIB compliance costs by streamlining CMMC requirements across DoD.

Our associations strongly disagree with the proposed rule's assertion at DFARS 204.7501(c) that the CMMC assessments would "not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements."[27]

The DIB is subject to audits and inspections from multiple DoD organizations. These audits and inspections are used to verify that a contractor implements similar security requirements that the CMMC framework is designed to achieve. Our associations recommend that DoD update the rulemaking to state, "The CMMC Program is the sole DoD assessment to verify a contractor's compliance with applicable DoD information security requirements." Absent this clarification, contractors would face burdensome and duplicative assessments, audits, and/or inspections from many DoD organizations.

[26] https://www.acquisition.gov/far/52.219-9
https://www.acquisition.gov/far/52.219-9#FAR_52_219_9__d3281e126

[27] *FR*, p. 66330.

8. Push for harmonization and reciprocity between CMMC and other cyber certification programs.

The White House and Congress have both made harmonization of cybersecurity regulatory regimes a priority for the federal government. The goals of this effort are to achieve better cybersecurity outcomes while lowering costs to businesses and their customers, including the U.S. government. The Office of the National Cyber Director (ONCD) studied the concerns of overlapping and conflicting cybersecurity governance structures over the past year through a request for information, which resulted in an assertion that the "lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs through additional administrative burdens."[28]

In July 2024, Homeland Security and Governmental Affairs Committee Chairman Gary Peters (D-MI) and Sen. James Lankford (R-OK) introduced S. 4630, Streamlining Federal Cybersecurity Regulations Act,[29] which creates a structure to align cybersecurity and information security examinations, regulations, and other compliance requirements set forth by many federal agencies. The committee passed the bill on July 31.[30] To proactively address these recognized burdens, our associations recommend that DoD introduce an ongoing process to achieve harmonization and/or reciprocity between obligations such as the FedRAMP certification standards and the CMMC Program.

In addition, the Canadian government has constructively initiated the development of the Canadian Program for Cyber Security Certification (CP-CSC), a new contracting security framework closely aligned with CMMC. The CP-CSC is designed to enhance the protection of sensitive, unclassified information held by Canadian defense contractors, bolstering Canada's cyber resilience. Moreover, the program seeks to minimize industry burden by pursuing mutual recognition with CMMC, enabling certified Canadian and American contractors to be acknowledged in both jurisdictions.[31]

9. Maintain the scope of safeguarded CDI and FCI under the CMMC Program.

The existing DFARS 252.204-7012 clause uses the defined term "Covered Defense Information" (CDI) that DoD contractors are familiar with, but the proposed DFARS 252.204-7021 rule does not use this defined term and instead uses CUI. The lack of alignment between CDI and CUI is confusing to many in industry. The definition of CDI in DFARS 252.204-7012 indicates that CDI is a subset of CUI—that is, CDI is DoD CUI provided to or

---

[28] ONCD, *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information*, June 2024, p. 5.
https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf

[29] The U.S. Chamber of Commerce supports S. 4630.
https://www.congress.gov/bill/118th-congress/senate-bill/4630

[30] https://www.hsgac.senate.gov/hearings/business-meeting-24

[31] "Canadian Government Urges DOD to Establish Reciprocity Between CMMC and Canadian Cyber Certification Program," *Inside Cybersecurity*, March 19, 2024.
https://insidecybersecurity.com/share/15655
https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2024/mar/cs2024_0074.pdf

collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

But the lack of alignment could also be interpreted to mean that the scope of information on a contractor's information system covered under the DFARS 252.204-7021 rule is much larger than the scope of information on a contractor's information system covered under DFARS 252.204-7012 pertaining to CDI and FCI.[32] However, such an interpretation would be contrary to DoD's statements indicating that the scope of information covered by CMMC Levels 1 and 2 are the same as the scope of information covered by FAR 52.204-21 and DFARS 252.204-7012. For example, DoD explicitly excluded from its cost estimates in the proposed 32 CFR Part 170 rule the costs for DoD contractors to obtain CMMC Levels 1 and 2 on the theory that such contractors would already be subject to FAR 52.204-21 and DFARS 252.204-7012.

In light of the fact that the DoD contractors have been implementing DFARS 252.204-7012 -7012 for nearly a decade for CDI as defined under the clause, our associations recommend that DoD makes it clear that the CMMC Program covers CDI and FCI in line with the scope of the DFARS 252.204-7012 rule rather than covering a newly broad set of data.[33]

---

[32] A significant point about external service providers' (ESPs') scoping requirements needs to be brought to DoD's attention. The draft clause in the August 15, 2024, proposed rule at 252.204-7021(b)(6) suggests that a contractor must ensure all its subcontractors and suppliers meet the relevant CMMC level required for a subcontract. But the final CMMC Program rule, which was published on October 15, 2024, makes clear that contractors may use ESPs, including cloud service providers (CSPs), without automatically requiring them to meet a CMMC level, subject to certain conditions (see Table 4 on *FR*, p. 83233). Indeed, only ESPs that store, process, or transmit CUI or security protection data must be assessed as part of the contractor's CMMC assessment scope. CSPs that store, process, or transmit CUI need a FedRAMP Moderate authorization or the equivalent. Thus, to ensure consistency, DoD is urged to include "(if applicable)" at 252.204-7021(b)(6) and 252.204-7021(d)(2) as shown in the bolded blue text below.

> (6) Ensure all subcontractors and suppliers complete and maintain on an annual basis, or when changes occur in CMMC compliance status (see 32 CFR part 170), an affirmation of continuous compliance with the security requirements associated with the CMMC level required for the subcontract or other contractual instrument **(if applicable)** for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract. . . .
>
> (d) Subcontracts. The Contractor shall—
> (1) Insert the substance of this clause, including this paragraph (d), and exclude paragraphs (b)(5) and (c), in subcontracts and other contractual instruments, including those for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items, when there is a requirement under the subcontract or similar contractual instrument for a CMMC level; and
> (2) Prior to awarding a subcontract or other contractual instrument, ensure that the subcontractor has a current CMMC certificate or current CMMC self-assessment at the CMMC level **(if applicable)** that is appropriate for the information that is being flowed down to the subcontractor.

FR, p. 66338.

DoD final rule, Cybersecurity Maturity Model Certification (CMMC) Program, *FR*, pp. 83092–83237, October 15, 2024. See "Table 4 to § 170.19(c)(2)(i)—ESP Scoping Requirements," *FR*, p. 83233.
https://www.federalregister.gov/d/2024-22905

[33] An organization told our associations, "CUI is used by other government agencies. For example, DHS [the Department of Homeland Security] issued its final rule [in June 2023] to implement security and privacy measures to safeguard CUI and improve incident reporting to DHS. DoD should clarify that the CMMC rules only apply to CUI that is subject to a DoD contract and not to other CUI information from non-DoD agencies."
https://www.federalregister.gov/d/2023-11270

10. Ensure that an information system processing FCI only needs CMMC Level 1.

The proposed language at DFARS 252.204-7021(b)(2) would require a contractor to "maintain the CMMC level required by the contract for the duration of the contract for all information systems, used in performance of the contract, that process, store, or transmit" FCI or CUI.[34] This language is not as clear as DoD may believe. It could be interpreted to mean that if a solicitation requires a CMMC Level 2 or higher in accordance with DFARS 252.204-7021(b)(1)(i),[35] then a contractor's information system that processes, stores, or transmits data limited to FCI, or Level 1, would also require CMMC Level 2. This interpretation would be at odds with the proposed CMMC Program at 32 CFR Part 170, which indicates that an information system that only processes FCI requires CMMC Level 1 and also allows contractors to use isolated enclaves within their environments to store FCI or CUI.

We urge DoD to bring this proposed DFARS 252.204-7021 language into line with 32 CFR Part 170 to ensure that an information system that processes FCI—but not CDI or CUI—only needs CMMC Level 1.

11. Permit contractors to define the scope of an information system applicable to the DoD unique identifiers (UIDs) requirements.

DFARS 252.204-7021(c)(1) would require a contractor to submit to a CO the DoD UID(s) for each of the contractor information systems that process, store, or transmit FCI or CUI during performance of the contract that are posted in SPRS.[36] This language is insufficiently clear whether a contractor must provide DoD UIDs only for its own information systems and those of its subcontractors. We presume that the former interpretation is correct because the proposed rule at 252.204-7021(d) specifically instructs contractors to "*exclude* paragraphs (b)(5) and (c)" [emphasis added] with regard to DoD UID requirements when flowing the substance of the clause to subcontractors.[37]

Our associations recommend that DoD clarify its rulemaking to ensure that contractors must provide DoD UIDs only for a contractor's own information systems. We also recommend specifying more clearly the scope of an information system that is associated with the DoD UID requirements. For example, an information system often refers to discrete information resources (e.g., hardware and software) that collects and processes data.[38] Or it could refer to an amalgam of information systems (e.g., a company's global information technology ecosystem), but only a part of the information system processes, stores, or transmits FCI and/or CUI. We urge DoD to

---

[34] *FR*, p. 66338.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] The National Institute for Standards and Technology refers to an information system as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." https://csrc.nist.gov/glossary/term/information_system

expressly permit contractors to define the scope of an information system that is governed under the DoD UID requirements. This approach is similar to the one developed by the Cybersecurity and Infrastructure Security Agency to facilitate software providers' attestations to the government concerning the Secure Software Development Framework.[39]

12. Absent a safe harbor, eliminate affirmations of compliance by a senior company official from the rulemaking.

The preamble of the proposed rule states that a "senior company official" must annually complete and maintain an affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS for each DoD UID applicable to each contractor information system.[40] However, there is no definition of the term "senior company official" at 32 CFR 170.4 (acronyms and definitions). DoD's proposal at 32 CFR 170 only states that a "senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements after every assessment, including POA&M [plan of action and milestones] closeout, and annually thereafter."[41] Moreover, the term senior company official does not appear in the proposed DFARS 252.204-7021 clause.

To date, the term "affirmation" has not been used in DoD contracts. Representations exist and are operational in federal contract administration and management by authoritative regulation. Regulatory contract terms in accordance with FAR 2.101 in operation for an affirmation via a certification or representation should be used, thereby removing continuous compliance affirmations and 72-hour notifications requirements from the CMMC Program.

Absent the inclusion of a regulatory and legal safe harbor for contractors in the rulemaking, our associations urge DoD to remove the reference to a senior company official from the proposal. The wording around a senior company official is undefined and vague in its applicability to contractors and subcontractors, including because of the absence of the term in DFARS 252.204-7021 and its implications for industry.

The area of cybersecurity has numerous examples of FARs or DFARS rules requiring contractors to make various certifications or representations regarding their compliance with agency requirements without specifying that a senior company official affirms compliance. FAR 52.204-21, for example, requires contractors to make certain representations regarding specific telecommunications and video surveillance services when making an offer to an agency.[42] Similarly, DFARS 252.204-7019 requires contractors to implement NIST SP 800–171 to be

---

[39] CISA, "Secure Software Development Attestation Form," March 18, 2024. https://www.cisa.gov/resources-tools/resources/secure-software-development-attestation-form

[40] *FR*, p. 66335.

[41] *FR*, p. 89060.

[42] FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems. https://www.acquisition.gov/far/52.204-21

considered for an award.[43] DFARS 252.204-7019 also includes a mechanism allowing contractors to submit self-representations of such assessments to the government without requiring a senior company official's affirmation for each assessment.

***

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.

American Foundry Society (AFS)
Associated Builders and Contractors (ABC)
BSA | The Software Alliance
Construction Industry Round Table (CIRT)
Industrial Fasteners Institute
National Association of Wholesaler-Distributors (NAW)
National Defense Industrial Association (NDIA)
Security Industry Association (SIA)
U.S. Chamber of Commerce

[43] DFARS 252.204-7019 Notice of NISTSP 800-171 DoD Assessment Requirements.
https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements

APPENDIX

Excerpted below is text from the U.S. Chamber's July 2024 letter to CISA on the notice of proposed rulemaking (NPRM) to implement CIRCIA reporting requirements.[44] The essential point is that the threshold for reporting a substantial cyber incident is too low and needs to be elevated to prevent overreporting by industry and overwhelming CISA with a flood of data. The CMMC Program's 72-hour notification requirement faces an identical problem.

Also important, DoD should prioritize cyber incident reporting harmonization and the establishment of CIRCIA agreements between CISA and DoD. The Chamber believes that cyber incident reporting harmonization and the establishment of CIRCIA agreements should be a priority for CISA and DoD. Worth recalling, lawmakers advocated for CIRCIA as a way for covered entities to avoid unnecessary burdens and harmonize duplicative cyber incident reporting regimes. In an overview document on CIRCIA, lawmakers plainly stated, "**An entity only has to report to Federal agencies once.** [Emphasis added.] If a covered entity is already required by law, regulation, or contract to report 'substantially similar' information on a substantially similar time frame to another Federal agency, it does not have to report to CISA."[45]

***

PROPOSED AMENDMENT TO THE DEFINITION OF A SUBSTANTIAL CYBER INCIDENT

Many in the business community believe that the definition of a *substantial* (or *covered*) *cyber incident* is overly broad and needs to be refined to (1) better align it with the intent of Congress in writing CIRCIA, (2) be more risk based, and (3) enhance reporting efficiency and security outcomes for industry and government.

The Chamber has three core concerns with the NPRM's definition of a substantial cyber incident:

First, unlike the term significant cyber incident, the word substantial is not defined in CIRCIA. The Chamber stressed to lawmakers that the word substantial would be unworkable in practice. Substantial is problematic because it could be interpreted by CISA to label almost any cyber incident as reportable.

Second, the authors of CIRCIA did not want CISA to be overwhelmed with a flood of unusable cyber incident data because of overly broad and prescriptive reporting by covered entities.

Third, to enhance reporting efficiency, a substantial cyber incident should be triggered only when there is a reasonable likelihood of a significant incident or harm to U.S. economic and

[44] https://www.regulations.gov/comment/CISA-2022-0010-0298

[45] Senate Homeland Security and Governmental Affairs Committee paper, "Peters-Portman Cyber Incident Reporting Act Overview," circa September 30, 2021.

national security. The Chamber believes that substantial cyber incidents should be limited to significant incidents that directly disrupt the operation of U.S. infrastructure owned or operated by a covered entity—the point being that the bar should be set high for the types of incidents that CISA would determine to be reportable.[46]

The government and industry require clearer definitions and higher reporting thresholds for the CIRCIA rule to work. The Chamber's amendment to the definition of a substantial cyber incident would ensure that a reportable incident is specifically tied to a "demonstrable harm to the national security interests, foreign relations, or economy" of the U.S. Further, the "demonstrable harm" wording is tied to an existing definition (i.e., a significant cyber incident, which refers to a "cyber incident that is . . . likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[47]

What is more, a demonstrably harmful cyber incident would likely be confirmable. Many in industry believe that reporting should be attached to confirmed cyber incidents. A 2021 letter to Congress signed by more than 30 associations states, "Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed [not potential] cyber incidents. . . . Covered cyber incidents should be attached to clear, objective criteria in legislation and any rule that agency and industry stakeholders develop."[48]

The insertion of *critical* in prongs (1) through (3) modifies the business/industrial operations, goods/products or services, information systems, or processes that are central to alerting CISA to cyber risks and developing mitigation strategies. The Chamber's proposed changes consider and support the factors listed in CIRCIA § 681b(c)(2).[49] Our recommended changes to the definition of a substantial cyber incident would constructively set the threshold for what constitutes a reportable cyber incident.

The NPRM's Proposed Definition of a Substantial Cyber Incident

Substantial cyber incident means a cyber incident that leads to any of the following:

[46] CIRCIA calls on CISA to conduct a review of a significant cyber incident, which includes a covered cyber incident and/or a ransomware attack, to identify and disseminate ways to prevent or mitigate similar incidents in the future. 6 U.S. Code (or CIRCIA) § 681a(6).

[47] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[48] https://www.uschamber.com/security/cybersecurity/coalition-letter-cyber-incident-reporting

[49] A firm told the Chamber that "entities should only be subject to mandatory reporting for their critical functions. CISA's NPRM suggests that an entire entity, not just an individual facility or function performed by an entity, would be covered under the reporting mandate. However, CISA's approach seems to ignore its own work on National Critical Functions that identified 'the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.'" The firm noted, "This work confirms that entities may have operations that are critical and those that are not. As such, entities should only be subject to mandatory reporting for their critical functions." https://www.cisa.gov/topics/risk-management/national-critical-functions

(1) A substantial loss of confidentiality, integrity or availability of a covered entity's information system or network;

(2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

(3) A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;

(4) Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:

(i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

(ii) Supply chain compromise.

(5) A "substantial cyber incident" resulting in the impacts listed in paragraphs (1) through (3) in this definition includes any cyber incident regardless of cause, including, but not limited to, any of the above incidents caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

(6) The term "substantial cyber incident" does not include: . . . .[50]

***

The Chamber's Proposed Revisions (Blue Text) to the Proposed Definition of a Substantial Cyber Incident in the NPRM

(1) A substantial loss of confidentiality, integrity or availability of a critical portion of a covered entity's information system or network required for the provision of critical products or services by that entity;

(2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes required for the provision of critical products or services by that entity;

(3) A disruption of a covered entity's ability to engage in a critical portion of business or industrial operations, or deliver critical goods or services;

(4) Unauthorized access and interruption, disruption, or destruction of ~~to~~ a covered entity's information system or network~~, or any nonpublic information contained therein,~~ that results in demonstrable harm[51] to the national security interests, foreign relations, or economy

[50] https://www.federalregister.gov/d/2024-06526/p-1623

[51] The NPRM states, "The plain language that Congress used throughout CIRCIA reflects the purpose discussed in CIRCIA's legislative history. For example, CIRCIA requires CISA to review covered cyber incidents that are 'likely to result in **demonstrable harm to the national security interests, foreign relations, or economy of the United States** [emphasis added] or to the public confidence, civil liberties, or public health and safety of the people of the United States' and to 'identify and disseminate ways to prevent or mitigate similar incidents in the future.' 6 U.S.C. 681(9); 6 U.S.C. 681a(a)(6). CIRCIA also requires CISA to 'assess potential impact of cyber incidents on public health and safety,' and to consider, when describing covered entities, both 'the consequences that disruption to or compromise of [a covered entity] could cause to national security, economic security, or public health and safety' and 'the extent to which damage, disruption, or unauthorized access to such an entity . . . will likely enable the disruption of the reliable operation of critical infrastructure.' 6 U.S.C. 681a(a)(1); 6 U.S.C. 681b(c)(1)(A), 681b(c)(1)(C)."
https://www.federalregister.gov/d/2024-06526/p-292

of the United States or to the public confidence, civil liberties, or public health and safety that is facilitated through or caused by a:

(i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

(ii) Supply chain compromise.

(5) A "substantial cyber incident" resulting in the impacts listed in paragraphs (1) through (3) in this definition includes any cyber incident that results in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety[52] regardless of cause, including, but not limited to, any of the above incidents caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

[52] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident