THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

SEPTEMBER 18, 2024 | VOLUME 66 | ISSUE 34

¶ 247 FEATURE COMMENT: The New Madness? CMMC-Mania—It's Arrived!

Just over 60 years ago, on Feb. 7, 1964, the Beatles touched down in America and made their live debut on the Ed Sullivan Show two days later. The event shook culture, but everyone knew it was coming. In fact, in little-known lore, the Beatles actually first appeared on American television months before through a four-minute segment on NBC's Huntley-Brinkley Report on Nov. 18, 1963. Nonetheless, their live arrival on Ed Sullivan triggered shockwaves worldwide, so much so that Time Magazine covered the growing "Beatlemania" in an article headlined "The New Madness." Similarly, but much less melodically, today, an event that debuted in the past and that everyone knew was coming has finally touched down: the Cybersecurity Maturity Model Certification (CMMC) Program. And while the arrival of CMMC may not carry the same kind of swooning favor as the Fab Four for defense contractors, it may result in a like-cultural earthquake capable of redefining the contracting industry, much like the Beatles transformed the music industry and captivated an entire generation.

On Aug. 15, 2024, the Department of Defense published proposed amendments to the Defense Federal Acquisition Regulation Supplement in the Federal Register (89 FR 66327), Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (Proposed Rule), unveiling more specifics on the long-awaited rollout of CMMC 2.0. Furthering the rule establishing the requirements of the CMMC Program at 32 CFR pt. 170, proposed on Dec. 26, 2023, the proposed amendments allow DOD to continue beating the cybersecurity drum and enhance data protection throughout the DOD supply chain through several changes to the DFARS, such as:

1) Adding/refining key definitions to the DFARS;

2) Formally incorporating the December 2023 CMMC 2.0 requirements;

3) Establishing a solicitation provision and prescription; and

4) Revising the existing DFARS 252.204-7021 clause language and prescription to reflect CMMC 2.0.

Just as the Beatles brought a fresh sound that shook up the music world, CMMC 2.0 and this Proposed Rule appear ready to revolutionize how cybersecurity is managed across the DOD supply chain. More than ever, with CMMC becoming increasingly set in stone and with the Proposed Rule's comment period ending on Oct. 15, 2024, federal contractors need to be prepared to rock if they want to stay on the DOD rolls.

The Arrival of CMMC 2.0: Hello, Goodbye—Back in 2019, DOD decided it was time to move away from the "self-attestation" model of security and pursue something more akin to "A Hard Day's Night" of rigorous standards to safeguard national security. So, under the guidance of the Office of the Under Secretary of Defense for Acquisition and Sustainment, the idea of CMMC was conceived to help protect the Defense Industrial Base (DIB) from the ever-evolving threats that were "Getting Better" every day.

By September 2020, DOD published an interim rule that made the industry twist and shout. This rule—Defense Federal Acquisition Regulation Supplement (DFARS): Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)—unveiled DOD's initial vision for what would be known as "CMMC 1.0." Defense Federal Acquisition Regulation Supplement Case 2019-D041. It laid out the basic beat of the program: a tiered model of cybersecurity practices and processes, required assessments, and implementation through contracts to keep Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) secure. This interim rule became effective on Nov. 30, 2020, kicking off a proposed five-year magical mystery tour of phased implementation.

But as the comments poured in—about 750—DOD knew it needed to "Come Together" again for a rethink. By March 2021, DOD started an internal review of CMMC 1.0. After a lot of listening and some help from its DIB friends, DOD announced the arrival of "CMMC 2.0" in November 2021. This new and improved version was designed to achieve the goals set out in the internal review, focusing on collaboration, accountability, and evolving cybersecurity measures.

Then, on Dec. 26, 2023, DOD fleshed out CMMC 2.0 through a proposed rule published in the Federal Register (88 FR 89058). The December proposed rule created a new 32 CFR pt. 170 to "establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors have … implemented required security measures [to safeguard sensitive unclassified information.]" It addressed certain policy problems identified by DOD, including how to verify contractor cybersecurity requirements, implement cybersecurity requirements by specifying the required CMMC level in the solicitation, and address scaling challenges by utilizing a private-sector accreditation structure.

Paperback Writing: New Definitions, Amendments, and Provisions—A constant and correct concern/complaint about cybersecurity efforts in federal contracting has been the lack of uniformity in definitions. Graciously, the Proposed Rule attempts to fix some of that by adding new definitions at DFARS 204.7501:

- CUI: Drawing from the definition in 32 CFR pt. 2002, this is set to provide a more specific picture of what needs to be protected.
- Current: This term relates to the present state of CMMC certificates, self-assessments, and affirmations of continuous compliance—ensuring everyone stays in tune.
- DOD Unique Identifier (DOD UID): A unique identifier and a "Ticket to Ride" within the Supplier Performance Risk System (SPRS) given to each contractor assessment.

The Proposed Rule also makes changes to DFARS 204.7502, Policy, requiring and clarifying that at the time of award, every contractor must have a "current" CMMC certificate or self-assessment for any system processing, storing, or transmitting FCI or CUI. Contractors can work it out only by ensuring they maintain that certificate or assessment throughout the contract's life.

New "Day Tripper"-style checklist requirements were added at DFARS 204.7503, Procedures. The Proposed Rule directs contracting officers to ensure

that the required CMMC level is included in solicitations and contracts. Before a contract award, option exercise, or when a new DOD UID pops up, the CO will need to verify in SPRS that the contractor possesses the following:

- A "current" CMMC certificate or self-assessment at or above the required level posted in SPRS for each DOD UID relevant to the systems handling FCI or CUI.
- A "current" affirmation of continuous compliance with the security requirements found in 32 CFR pt. 170 in SPRS for each applicable DOD UID.

Another "Here Comes the Sun" addition is the new proposed DFARS Provision, 252.204-7YYY, intended to let offerors know the required CMMC level for the solicitation. Moreover, it is also intended to ensure that the winning offeror has posted their CMMC certificate or self-assessment results in SPRS before the contract is awarded.

Beyond the specific additions, the Proposed Rule also includes various conforming changes across the DFARS to ensure that the new CMMC 2.0 requirements are harmoniously integrated into existing regulations. For instance, DFARS 212.301 has been amended to include the new provision 252.204-7YYY, "Notice of Cybersecurity Maturity Model Certification Level Requirements," ensuring that all parties know the CMMC levels required. Similarly, DFARS 217.207 now advises COs to verify CMMC compliance before exercising any contract options.

Revolution: Changes to DFARS 252.204-7021—You say you want a real solution? Well, the Proposed Rule also tells us of an evolution of the existing CMMC clause at DFARS 252.204-7021, now titled Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements. The clause is expected to appear across the universe of DOD contracts, task orders, or delivery orders that require the contractor to have a CMMC certificate or CMMC self-assessment at a specific level. Importantly, this includes contracts for commercial products and services except, as we've seen before, those contracts exclusively for commercially available off-the-shelf (COTS) items. While this clause has been on the books since January 2023, it has been a bit of a "Nowhere Man" as the DOD has been busy fine-tuning the CMMC requirements. But now, with the Proposed Rule, some new harmonies are being added to the tune:

- Keep Your CMMC Level Up to Snuff: Just like "Here, There, and Everywhere," contractors must maintain the right CMMC level for the entire contract life. Every system that processes, stores, or transmits FCI or CUI needs to be covered, no matter where you are.
- Stay on the Right Track with Data: When transmitting data on systems that handle FCI or CUI, "All You Need is" the right CMMC certificate or self-assessment at the level required by the contract. No shortcuts, just a steady beat of compliance.
- A Little Help from Senior Officials: A "senior company official" must complete an affirmation of continuous compliance with the security requirements of 32 CFR pt. 170. This needs to happen every year, and anytime there's a "security change"—keeping everything up to date.
- Speak Up When Things Go Wrong: If there's a lapse in information security or if your CMMC certificate or self-assessment levels change during the contract, it's time to "Get Back" to the CO and the DIB within the well-known 72-hour window.
- Make Sure Your Subcontractors Are In Harmony: Before you shake it up with any subcontractors, make sure they're singing the same tune at the right CMMC level. This means checking in with 32 CFR pt. 170 for guidance and ensuring the requirements flow down as required.

Phased Rollout: The Slow Build to a Cultural Shift—Just as Beatlemania didn't take over America overnight, DOD is implementing CMMC 2.0 through a phased rollout over three years, ideally starting in 2025. During this period, contractors must meet specific CMMC levels before processing, storing, or

transmitting FCI or CUI, as determined by the program office or requiring activity. During that period, the Government will have some homework to fine-tune their processes in line with the finalized version of 32 CFR pt. 170 and understand how to implement if/how CMMC gets added to a contract. That, for sure, will be a long and winding road, but after this three-year phase-in period, every DOD solicitation and contract valued above the micro-purchase threshold that's dealing with FCI or CUI will need to have a CMMC level from commercial products to commercial services—unless it's COTS items.

Subcontractor Flow-Down: Don't Let Me Down—In the same way that the Beatles influenced countless other bands, CMMC 2.0 mandates that contractors ensure their subcontractors meet the required cybersecurity standards. Just as the Beatles' sound spread and inspired musicians across the globe, CMMC 2.0's requirements will flow down through every level of the defense supply chain. This ensures that cybersecurity standards are consistently applied across the board, like how the British Invasion reshaped the entire music industry.

Accordingly, ensuring subcontractor compliance with CMMC requirements is a repeating chorus in both the Proposed Rule and the December 2023 Proposed Rule, and their shared goal is to strengthen the protection of FCI and CUI throughout all tiers of the DOD supply chain. More granularity is needed, but the revised clause proposed at DFARS 252.204-7021 would require these CMMC obligations to flow down to subcontracts, including those involving commercial products and services if the subcontract involves meeting a specific CMMC level. Prime contractors will be responsible for determining the appropriate CMMC level for each subcontract, guided by their review of the requirements outlined in 32 CFR pt. 170 and, hopefully, guidance provided in the prime contact (fingers crossed). While the Proposed Rule references the December 2023 Proposed Rule for more details, feedback on that rule has highlighted concerns about how that process would play out.

Suffice it to say that there remains uncertainty around how prime contractors should identify and assign the correct CMMC level to their subcontractors. However, once the appropriate CMMC level is identified and assigned, a prospective subcontractor must have a current CMMC certificate or self-assessment at that required level before the subcontract is awarded. While this sounds straightforward on paper, the real-world application may be anything but. Prime and higher-tier subcontractors will face a learning curve as they navigate the requirements of 32 CFR pt. 170 to determine the correct CMMC level for each supply chain tier, which could lead to some confusion or resistance.

A complication that is sure to play on repeat in all comments is the fact that prime contractors do not have the ability to verify their subcontractors' CMMC status electronically. Acknowledging this challenge—but without providing a practical solution—DOD notes in the Proposed Rule that prime contractors are "expected to work with their suppliers to conduct verifications as they would under any other clause requirement that applies to subcontractors" (89 FR at 66331). While this might be seen as falling under the general responsibility of managing subcontractors, the proposed rules don't offer clear guidance on, if asked/investigated, how to effectively ensure these CMMC requirements will have been deemed to have properly flown down.

Help!: Contractor Compliance—Just as the Beatles had to innovate to maintain their relevance continually, contractors under CMMC 2.0 must affirm their compliance with cybersecurity standards on an ongoing basis. This isn't just a one-time certification—it's an ongoing process. Contractors must maintain their certification throughout the contract and report any changes in their cybersecurity posture to the CO. So, as there might be much work to do, let's provide a little bit of a Beatles playlist to help you through the effort:

1) "*I Want to Hold Your Hand*"—Understand CUI. Make sure to have a comprehensive CUI policy to address the overlay of CMMC requirements. Understanding that something needs to be protected but unable to identify it could lead many into a thick "Norwegian Wood" from which it may be hard to escape.

While at it, take some time to evaluate all existing cybersecurity policies, procedures, and technical controls against the practices and processes outlined in the CMMC model.

2) "*All Together Now*"—Build an Internal CMMC Team or Task Force. Establish an internal CMMC compliance team or task force comprising key personnel from information technology, cybersecurity, compliance, legal, and procurement departments. This team should oversee the CMMC compliance efforts and coordinate with external assessors or consultants. There is a dynamic area where contractors and subcontractors must keep up to date with any changes or finalization of the Proposed Rule and the December 2023 Proposed Rule. Regulatory changes may require adjustments to cybersecurity efforts, and staying informed will allow quicker adaption and adoption.

3) "*We Can Work It Out*"—Understand the Requirements of 32 CFR pt. 170. Although more CO-facing, contractors should thoroughly review the provisions in 32 CFR pt. 170 to become more familiar with the specific security requirements outlined for each CMMC-level (Levels 1, 2, and 3) and how these requirements apply to their organization *and* focus on understanding the processes for continuous compliance, reporting obligations, and the flow-down requirements to subcontractors.

4) "*I'm Looking Through You*"—Conduct a Gap Analysis. Perform a comprehensive gap analysis of your current cybersecurity posture against the requirements for the applicable CMMC level. Examine the status of pending Plans of Action and Milestones to identify areas that fall short of requirements and develop a plan to address these gaps. This will also allow companies to scope out the information systems that process, store, or transmit CUI and FCI that are in scope for the CMMC requirements.

5) "*The Long and Winding Road*"—Develop a Comprehensive CMMC Compliance Plan. A detailed and tailored CMMC compliance plan should outline each step required to achieve and maintain the required CMMC level, including timelines, responsible parties, budget considerations, and milestones. Moreover, it allows the company to align these requirements against broader business objectives and risk management strategies. As an added "B Side" bonus, a well-documented plan can help demonstrate cybersecurity commitment to the DOD customer, regulators, and prime/sub/teaming partners.

6) "*Fixing a Hole*"—Implement Required Security Controls. Based on the gap analysis and plan results, implement the necessary security controls to meet the required CMMC level for your contract. This may include technical measures (e.g., multi-factor authentication, encryption), policy updates (e.g., incident response plans), and personnel training. Ensure that these controls are not only implemented but also documented and maintained. Continuous monitoring, regular audits, and internal assessments should be part of any compliance strategy.

7) "*Getting Better*"—Prepare for Certification and Self-Assessments. Prepare for an official assessment by a CMMC Third Party Assessment Organization by ensuring all required documentation, evidence, and processes are in place for a successful assessment. This will also assist in contracts requiring a self-assessment, but be sure to do so honestly and maybe seek a reliable third party to assist. Remember, the Proposed Rule requires that a "senior company official," as defined in 32 CFR 170.4, sign off on the affirmation of continuous compliance. Maintain these records and update them annually or whenever significant security changes occur.

8) "*Come Together*"—Strengthen Supply Chain and Subcontractor Management. Develop a robust plan to ensure all subcontractors meet

the necessary CMMC level for the information they handle as part of existing subcontract plans. This includes incorporating appropriate subcontract clauses, verifying subcontractor certifications or self-assessments, and providing guidance to help them comply. A key factor here will be establishing continuous collaboration and communication processes with subcontractors to verify their CMMC status, address gaps, and manage compliance risks effectively.

9) "*Helter Skelter*"—Establish Incident Reporting and Response Mechanisms. Set up mechanisms to ensure existing incident response plans can comply with reporting requirements, such as notifying the CO within 72 hours of any lapses in information security or changes in the status of CMMC certification or self-assessment levels. This may also require that all staff are trained on the procedures for responding to and reporting cybersecurity incidents.

10) "*Eight Days a Week*"—Establish a Robust Continuous Monitoring Program. At the outset of CMMC, the "maturity" of an enterprise's cybersecurity stance was evaluated. While some of those requirements have faded, the general sentiment remains. Defense contractors should, therefore, implement a continuous monitoring program capable of performing regular checks for CMMC requirement compliance and have the ability to identify and address any security gaps, such as through vulnerability scanning, patch management, log review, and routine compliance audits.

"I Don't Want to Spoil the Party," but the rollout of CMMC 2.0 is more than just a regulatory update—it's the beginning of a new era in cybersecurity for DOD, as significant as the Beatles' arrival in America was for the music industry. Above all else, "A Day in the Life" of a DOD contractor following CMMC will require a committed culture of cybersecurity awareness. The good news is that no DOD contractor is a Lonely Hearts Club Band. There will be many questions and much confusion, so be prepared to ask questions—even if the answers may not be wanted. Ultimately, CMMC is not something that one can avoid or "Let It Be," or their customers, partners, and the Department of Justice will ask, "Tell Me Why."

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Alexander Major *and* Cara Wulf. *Ms. Wulf is a partner and Mr. Major is a partner and co-leader of the Government Contracts & Global Trade Practice Group in the Washington, D.C. office of McCarter & English, LLP. They can be reached at amajor@mccarter.com and cwulf@mccarter.com.