COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2024

Janet Himmelreich (janet.himmelreich@3comply.com, linkedin.com/in/janethimmelreichgrcexpert/) is a Managing Director of 3Comply LLC in King of Prussia, Pennsylvania, USA.

Are you an ostrich? For CMMC, you'd best be a roadrunner

By Janet Himmelreich, CIPP/E/US, CMMC RA, RPA, formerly CCEP

In the last issue, we discussed the fuss around the Cybersecurity Maturity Model Certification (CMMC).[1] Although the final regulations have recently been published establishing the CMMC validation program as a formal "program" for the U.S. Department of Defense (DoD), the long of it—it's been discussed since 2017—and the short of it—the effective date of the final rules is expected in Q1 2025—is now reality.[2] Many people had taken the position they would believe it when they see it. Well, here it is.

CMMC is designed to validate that the controls of NIST SP 800-171 Rev. 2 have been implemented.[3] An independent assessment demonstrates that the controls are implemented correctly, operating as intended, and that the required outcome can be evidenced. This validation is necessary for contracting with the DoD but also helps companies protect their intellectual property for any business operations. All supply chains are under attack from cybercriminals, and the safer your information and data are, the better off you will be.

Many companies in the defense industrial base preferred that security achievements— particularly ISO 27001 certification and/or SOC 2 attestation—be used in place of CMMC validation. These activities are considered significantly different by the DoD and, thus, are not acceptable. However, the good news is if you have achieved either or both, your environment is significantly advanced relative to a company with no security framework compared to the controls of NIST SP 800-171. At the end of the day, any security frameworks, whether from NIST or another entity, cover people, processes, and systems—not just technology. It is key that the people involved are trained, knowledgeable of the processes and procedures, and able to demonstrate compliance to an auditor or an assessment team. As is true for any framework a company must comply with, it is *always* about the people.

Rulemaking statuses

The DoD published its final proposed rules for the *program* of CMMC on December 26, 2023. The public comment date closed on February 26, 2024, and so far, the website for collecting and reporting on the comments states that there are almost 800 comments received by the end of the first week in March.[4] Thus far, 368 comments have been made available through the docket. The next step in rulemaking is publication of the final proposed rules under 48 C.F.R. Chapter 2, which will define the *acquisition* rules that need to be refined to reflect the program as defined in 32 C.F.R. § 170.[5] DoD spokespersons said the rulesets are expected to have the same effective dates: after the 60-day comment period expected for the revised Defense Federal Acquisition Regulation Supplement (DFARS) rules when published. (The February 9, 2024, Regulatory Flex Agenda pointed to the link for weekly updates by the DoD regarding open cases).[6] As of March 8, 2024, the proposed DFARS regulations were still described as: "02/23/2024 Case manager forwarded draft proposed rule to DARS Regulatory Control

Officer. DARS Regulatory Control Officer reviewing."[7] Based on the Fall 2023 Regulatory Agenda, most pundits expected that the DFARS rules would be published in March 2024. As of April 15, 2024, the rules have not been published. This is crucial, as both pieces are needed prior to the rules going into effect.

The DoD promised a statement before the end of the comment period for 32 C.F.R. § 170; a video statement was released on February 7, 2024.[8] It seems the philosophy was that a picture is worth a thousand words. The video reiterates many of the statements found in the body of the proposed rules from December 2023, but it may make some of the requirements a bit clearer than if one were to simply follow the written mass of words.

It is worth noting that CMMC and the DFARS 254.204-7012 procurement clauses refer to NIST SP 800-171 Rev. 2, which only addresses *nonfederal* systems use. Thus, this applies to situations where the contractor provides and uses its own systems. If a contractor provides systems to the federal government that *it* uses, then these cybersecurity requirements can be found in NIST SP 800-53 Rev. 5b.[9] This is the set of requirements that drive the smaller number of requirements found in NIST SP 800-171 Rev. 2.

Two assessments?

Companies with both federal contract information (FCI) and controlled unclassified information (CUI) appear to need two assessments, but that's something that needs to be clarified. The following descriptions are imported from the November 2023 *CMMC Model Overview* from the DoD. This and seven other documents were published along with the proposed rule.[10] These documents reflect CMMC 2.0 and are not expected to change when the rules become "final." Of note is that NIST SP 800-171 Rev. 2 is actually codified in the proposed program rules.[11] This has been a major topic of concern, as NIST is just about ready to release version 3 of NIST SP 800-171. There are *a lot* of items still in play!

A close read of the following definitions demonstrates that Level 1 now refers directly to the Federal Acquisition Regulation (FAR) clause and its 15 basic requirements. This is a change from the guidance from November 2021. The codes for the 15 controls are very different; they refer to the FAR clause 52.204-21.

Up until the release of the updated guidance—including the scope and assessment documents—most people proceeded assuming a Level 2 assessment (all 110 controls) would also satisfy the requirements of a Level 1 assessment since the Level 1 controls were encompassed in the Level 2 controls. This does not appear to be the case.

> CMMC Level 1
>
> Level 1 focuses on the protection of FCI and consists of the requirements that correspond to the 15 basic safeguarding requirements specified in 48 CFR 52.204-21, commonly referred to as the FAR Clause.
>
> CMMC Level 2
>
> Level 2 focuses on the protection of CUI and incorporates the 110 security requirements specified in NIST SP 800-171 Rev 2.
>
> CMMC Level 3
>
> Level 3 focuses on the protection of CUI and encompasses a subset of the NIST SP 800-172 security requirements with DoD-approved parameters. DoD-approved

> parameters are denoted with underlining.[12]

Note that there had not been any definition of Level 3 until these documents were released.

As a reminder, the Level 1 information being protected as FCI is defined in 32 C.F.R. § 170.4 and 48 C.F.R. § 4.1901:

> Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments.

CUI (pronounce it however you like, as long as you know what it stands for!) is the focus of Levels 2 and 3 and is defined in 32 C.F.R. § 2002.4(h) as:

> [. . .] information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

The tier descriptions are found on page four of the *CMMC Model Overview*.[13] There has been conjecture about the fact that different assessments, also resulting from the rollout phases, will be required. We will examine those next.

Phased rollout of CMMC 2.0

The three tiers of CMMC in the proposed rule are the same under CMMC 2.0. Level 1 is the most basic and points solely to the FAR 52.204-21(b) descriptions of 15 basic cybersecurity hygiene requirements. Because this is so basic, it is directed only at contractors processing, storing, or transmitting FCI. At this level, all DoD contractors *must* affirm compliance by a senior official via the Supplier Performance and Risk System (SPRS) account with the DoD. Phase 1 of the rollout is the self-assessment period for CMMC, which likely applies to every DoD contractor.

Surprise, surprise to many contractors: The Level 1 *Self-Assessment Guide* (which is based on NIST SP 800-171A even though the control requirements are from FAR 52.204-21) sets out specific items that need to have been completed for a senior official to affirm compliance.[14] It requires a score and a self-assessment report that follows the guidance on how to determine if items are in compliance, including:

- Scope (per the Level 1 *Scoping Guide*) applicable to processing, transmitting, or storing FCI
- Defined boundaries
- Method, which includes use of "Examine, Interview, and Tests" as prescribed in NIST SP 800-171A
- Assessment of each objective from the NIST SP 800-171A guidance related to the 15 controls of FAR 52.204-21, with a notation of what evidence was available and whether it was sufficient to meet the objective of protecting the FCI by a determination of "MET" or "UNMET" (nonapplicable is possible as well)

Any objective that cannot be met during assessment must be remediated before the report can be finalized. At Level 1, there are no allowances for a Plan of Action and Milestones.

When the self-assessment is completed, the designated senior official needs to enter the score in SPRS and post the completed report. Again, all items must be met, so only a perfect score may be entered. The self-assessment requirement phase (i.e., when a procurement or contract officer may require a self-assessment at Level 1—or a Level 2 if, in their view, that is acceptable) comes into effect as soon as the revised DFARS requirements are final, and then it lasts for six months. Others with more connections than me have calculated that this could be as soon as October of this year (although more likely Q1 2025). Please note that self-assessments are due annually, and *all* must be conducted as previously described.

The following table—developed by SheppardMullin for its blog—is helpful to understand the two-and-a-half-year rollout plan:[15]

Phase	Start Date	Impact
Phase 1	On the date CMMC revisions to the DFARS become effective (DFARS case 2019-D041).	Inclusion of CMMC Level 1 or CMMC Level 2 Self-Assessment requirement in applicable solicitations/contracts (as a condition of award).
Phase 2	Six months after Phase 1 begins.	CMMC Level 2 Certification Assessments (*i.e.*, C3PAO assessments) in applicable solicitations/contracts (as a condition of award).
Phase 3	One calendar year after Phase 2 begins.	CMMC Level 2 Certification Assessment for exercising option periods; and CMMC Level 3 Certification Assessment for all applicable solicitations/contracts (as a condition of award).
Phase 4	One calendar year after Phase 3 begins.	Full implementation of the CMMC requirements in all applicable solicitations and contracts, including option periods on contracts.

Regardless of the rule's effective date, the DoD notes in the proposed rules that it "intends to include CMMC requirements for Levels 1, 2, and 3 in all solicitations issued on or after October 1, 2026, when warranted by any FCI or CUI information protection requirements for the contract effort."[16] Of note is that individual DoD program managers will be able to require CMMC at a specific level *before that time*. This seems to match with our experience in that CMMC requirements are being found in solicitations *now*. Prime contractors are also pushing them on to their subcontractors.

Better start now

The rules may *say* October 2026 is the required date, but in reality, there will continue to be a major push for NIST SP 800-171 compliance from anyone with an SPRS account and a DoD contract containing the procurement clause 254.202-7012. This requirement has been in force since 2017, and the risks of cyberattacks for all companies—particularly small ones—continue to increase exponentially. The DoD has begun examining SPRS scores and reviewing the contractor's conduct via anything from a desk audit to a full on-site audit. If you are an ostrich, have had your head in the sand, and are in the "senior official" group, you have great cause for concern.

Many companies took the approach that they needed a high SPRS score to be awarded contracts, and in fairness, the DoD wasn't doing much enforcement, so the highest score of 110 was entered. While some might have knowingly done this, there were others who truly thought they must have a perfect score since they had spent so much time and money on their IT systems. Even today, procurement officers are fully willing to ignore the NIST SP 800-171 score.

Thus, there are a good number of the approximately 220,000 members of the defense industrial base that either have a defensive reason to seek CMMC certification or want a competitive advantage by having CMMC certification earlier rather than later.[17] To date, there are 54 assessments that have been completed jointly with the DoD and a total of 188 candidates in the pipeline as reported by the Cyber AB in its February 27, 2024, town hall.[18] Cyber AB is the nonprofit company holding the DoD contract to perform the assessments and provide the training required for CMMC assessors, as well as other roles named in the proposed rules. Additionally, it oversees registered practitioners who are the implementers in the ecosystem. Assessors cannot have worked with an organization on implementation and then assess it as you would expect. This pales in comparison to the nearly 77,000 companies the DoD estimates will seek Level 2 certification.[19]

Most industry pundits, including myself, believe that number is a huge undercount. One big reason is that even if a contractor has a requirement from a prime contractor for FCI information only—and thus, CMMC Level 1—most companies do not want to be constrained by only having a Level 1 self-assessment. Another reason is that many companies really do not believe the DoD will fully educate its staff to the requirements. There's a risk that having a low self-assessment score will thwart their chances of winning, so certification would be preferred. There is also the "small" matter that the proposed rules now require managed service providers and managed security service providers—known as external service providers (ESPs)—to hold the same CMMC level as their client(s). This is one of the big surprises from the proposed rules and significant clarification will need to be provided before they are finalized. There is no estimate of how many of these companies there are, but we can expect it to be fairly substantial; companies of all sizes tend to use an ESP to assist with IT services.

Once the rules are in full force and effect (or at least by October 1, 2026), the specifications for a*new* contract require that the CMMC level specified be a condition of award. The proposed rules made this official, and it could be applied to any options remaining on in-place contracts.

You'd better become a roadrunner!

The DoD estimates it could take 18 months to two years to complete the environment required for CMMC compliance if starting from “new.” Most companies are probably not starting from new, as it has been prudent to protect personally identifiable information as well as intellectual property by instilling and installing at least basic levels of security in the organization. However, being able to *prove* the efforts are “implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization,” as defined in 32 C.F.R. § 170.15 through 32 C.F.R. § 170.18, may not have been in place.

Another item clarified in the proposed rules is that the CMMC requirements apply to *all* tiers in the supply chain. It doesn’t matter if you are a direct contractor to the DoD or a prime contractor or to a subcontractor of a prime—if you are in the supply chain of a DoD contract, the CMMC requirements apply to you. If you only have a little bit of information or are really small, you may consider yourself insignificant. The DoD does not. If they are ultimately the ones paying the bill, and you knowingly submit invoices with the intent to be paid even though you know you have not put all the required security controls in place, you open yourself and your company to a potential U.S. Department of Justice investigation under the False Claims Act. If you know how it has been used in healthcare, you can imagine how it might be used for DoD contractors! The results would scare pretty much anyone into putting on their roadrunner shoes and getting going on implementing CMMC requirements as soon as possible.

Takeaways

- Rulemaking and program requirements for Cybersecurity Maturity Model Certification (CMMC) are through public comments, and as of this writing, we anticipate the procurement rules any day now.
- Companies with both federal contract information and controlled unclassified information will likely need two assessments.
- The proposed rollout for CMMC 2.0 begins as soon as the program and procurement rules are final. Level 1 compliance is required in the first six months, and everything else has two years.
- The rules may *say* October 1, 2026, is the absolute effective date, but there are all sorts of reasons why there are requirements now.
- The horses have left the barn, and there are no exceptions; if you plan to or are doing business with the U.S. Department of Defense, you *must* comply.

[1] Janet Himmelreich, “What’s all the fuss about CMMC?” *CEP Magazine* (May 2024).
[2] Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. 89,058 (Dec. 26, 2023) (to be codified at 32 C.F.R. pt. 170), https://www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-27280.pdf.
[3] National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171 (rev. 2), February 2020, https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final.
[4] Department of Defense, “Cybersecurity Maturity Model Certification (CMMC) Program,” DOD-2023-OS-0063, Regulations.gov, accessed April 11, 2024, https://www.regulations.gov/docket/DOD-2023-OS-0063.
[5]48 C.F.R. § 200-299, https://www.ecfr.gov/current/title-48/chapter-2.
[6] Introduction to the Unified Agenda of Federal Regulatory and Deregulatory Actions—Fall 2023, 89 Fed. Reg. at 9,324 (Feb. 9, 2024), https://www.govinfo.gov/content/pkg/FR-2024-02-09/pdf/2024-00476.pdf.
[7] U.S. Department of Defense, Defense Federal Acquisition Regulation Supplement, “Open DFARS Cases as of 4/5/2024,” March 8, 2024, https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf.
[8] U.S. Department of Defense, Army Multimedia and Visual Information Division, “Cybersecurity Maturity Model

Certification (CMMC) Proposed Rule Overview," video, February 7, 2024, https://www.defense.gov/Multimedia/Videos/videoid/912871/.

[9] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 (rev. 5.1.1), November 2023, Nov. 7, 2023, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[10] U.S. Department of Defense, "CMMC Documentation," last accessed April 11, 2024, https://dodcio.defense.gov/CMMC/Documentation/.

[11]32 C.F.R. § 170, Section 14.

[12] U.S. Department of Defense, *Cybersecurity Maturity Model Certification (CMMC) Model Overview*, version 2.1, draft, July 2023, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2023/aug/cs2023_0167a.pdf.

[13] U.S. Department of Defense, *Cybersecurity Maturity Model Certification (CMMC) Model Overview*, version 2.0, December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf.

[14] U.S. Department of Defense, *CMMC Self-Assessment Guide; Level 1*, version 2.0, December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf.

[15] Townsend Bourne, Nikole Snyder, and Jordan Mallory, "New Year, New Rules: The CMMC Proposed Rule is Here," SheppardMullin Government Contracts & Investigations Blog, January 2, 2024, https://www.governmentcontractslawblog.com/2024/01/articles/defense-contracts/new-year-new-rules-the-cmmc-proposed-rule-is-here/

[16] Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. at 89,071, https://www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-27280.pdf.

[17] Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. at 89,071.

[18] Cyber AB, "CMMC March 2024 Town Hall," video conference, March 2024,https://cyberab.org/news-events/town-halls.

[19] Cybersecurity Maturity Model Certification (CMMC) Program, 88 Fed. Reg. 89,058, 89,085 (Dec. 26, 2023), https://www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-27280.pdf.