# DOD Clarifies Contractor Cybersecurity Certification — Again

By **Amy Conant Hoang, Erica Bakies and Sarah Burgart**

Amy Conant Hoang

Erica Bakies

Sarah Burgart

On Dec. 12, the U.S. Department of Defense publicly released an updated draft of the Cybersecurity Maturity Model Certification, or CMMC, framework, Rev 0.7. This draft follows a previous version released on Nov. 8 (Rev 0.6), which we assessed in a prior article.[1] While the latest draft provides much-needed detail on requirements for contractors who expect to be in the higher tiers of the CMMC's five level framework, it also leaves several information gaps unfilled.

**Key Takeaways**

For those already familiar with the CMMC basics, here are the key updates from the latest draft:

***What's New***

- Level 4 and 5 practices. Rev 0.7 includes practices that contractors must meet in order to be certified at Levels 4 and 5. Rev 0.6 only included the practices required for Levels 1–3.

- Explanations for Level 2 and 3 practices. Rev 0.7 includes appendices identifying Level 2 and 3 practices, including discussion and clarification for each practice and examples of practices being demonstrated within a company. Rev 0.6 included a similar appendix for Level 1 practices.

- New capabilities. Rev 0.7 adds three new capabilities to the model for a total of 43 capabilities across 17 domains.

- Fewer practices. The DOD has continued to pare down the number of practices required for each CMMC level. Rev 0.7 includes 173 practices across all five levels, a decrease from the 219 required in Rev 0.6 and the 340 required in Rev 0.4.

***What's Missing***

- Discussion and clarification appendices for Level 4 and 5 practices. We likely will not see these until the release of Version 1.0 in January 2020.

- Process requirements for each domain. Rev 0.7 continues to focus on practices without providing any additional information on processes. It includes the same nine processes that were included in Rev 0.6, and states that "Version 1.0 will include tailored maturity processes for each domain."[2]

The sections below provide more details on the changes across the three key components of the draft framework: the CMMC narrative, the CMMC model (Appendix A), and the explanatory appendices (Appendices B–F).

**CMMC Narrative Updates**

Although Rev 0.7's narrative description of the framework largely replicates the narrative in Rev 0.6, the current draft includes a handful of important changes that further clarify how the CMMC will function once implemented.

***Certification for Segments of Networks***

Rev 0.7 includes a new statement clarifying that a contractor may achieve a certification level either for its "entire enterprise network" or for "particular segment(s) or enclave(s)."[3] This indicates that contractors may not be required to implement CMMC practices and processes across their entire networks but rather only the specific part of the contractor's network that hosts federal contract information or controlled unclassified information.

***Compliance with Other Regulations***

Rev 0.7 reiterates that "organizations subject to DFARS clause 252.204-7012 will have to meet additional requirements such as incident reporting."[4] This statement reminds contractors that Defense Federal Acquisition Regulation Supplement reporting requirements have not been superseded by the CMMC.[5]

***To-Be-Determined Maturity Processes***

Rev 0.7 states that the final version of the model will include tailored maturity processes for each domain. The present and prior drafts have included only nine generic maturity processes across the five CMMC levels, and the processes are not specific to any domain.[6]

***Near-Final Version***

Rev 0.7 states that the DOD will release the final version of the framework at the end of January 2020. Rev 0.7 also indicates that the DOD is not expecting to make significant changes to the structure of the model ahead of the final release, in contrast to statements from prior versions such as the "model is still being refined" (Rev 0.4) and "this format may change ahead of the final version" (Rev 0.6). Rev 0.7 does not specifically solicit public comments on the framework.

**CMMC Model Updates**

Rev 0.7 provides two material updates to the CMMC model (Appendix A).

***1. Increase in the Number of Capabilities***

Rev 0.7 includes three new capabilities, defined as "achievements to ensure cybersecurity objectives are met within each domain."[7] As part of the asset management domain, the model includes a new capability entitled "manage asset inventory." Under the recovery domain, the model lists a new capability entitled "manage information security continuity." Finally, in the risk management domain, the model adds another capability entitled "manage supply chain risk."

2. ***Decrease in the Number of Practices***

As expected, Rev 0.7 significantly reduces the number of practices for Levels 4 and 5, following the previous reductions to the practices in Levels 1 through 3. Since the release of Rev 0.4 in September, the CMMC has decreased practice requirements by more than half, from 380 practices down to 173:

| Model Level | No. of Practices in Rev 0.4 (September 2019) | No. of Practices in Rev 0.6 November 2019) | No. of Practices in Rev 0.7 (December 2019) |
|---|---|---|---|
| Level 1 | 35 | 17 | 17 |
| Level 2 | 115 | 58 | 55 |
| Level 3 | 92 | 56 | 59 |
| Level 4 | 96 | -- | 26 |
| Level 5 | 42 | -- | 16 |

**Appendix Updates**

Rev 0.7 contains three primary updates to the CMMC appendices in addition to the updates to Appendix A, the CMMC model itself.

***1. Discussion and Clarification for Practices in Levels 2 and 3***

Rev 0.7 now includes appendices for discussion and clarification of the practices in Level 2 (Appendix C) and Level 3 (Appendix D), supplementing the appendix for Level 1 (Appendix B) included in Rev 0.6. These appendices detail: (1) the references from which the practice originated; (2) discussion of the practice (usually text pulled from the references, except for those practices that have no prior reference before the CMMC); and (3) clarification of the practice, including an example of how the practice would be demonstrated within a company.

The discussion and clarification appendix for Level 3 (Appendix D) excludes the 45 Level 3 practices taken from NIST 800-171 Rev 1 and includes discussion and clarification only for the remaining 14 practices that originated elsewhere, likely because the National Institute of Standards and Technology includes its own clarifications for these practices in 800-171 Rev 1.

***2. Discussion and Clarification for Processes***

Rev 0.7 includes a new Appendix E containing discussion and clarification for the nine maturity processes currently included in the CMMC model.[8] Appendix E provides the CMMC interpretation of the current process requirements such as "providing a policy," "establishing a plan," "providing adequate resources" and "standardizing an approach,"

which we assume will become the basis for the tailored processes we expect to see in Version 1.0.

### *3. Updates to the CMMC Definitions*

Rev 0.7 makes several minor changes to Appendix F, the CMMC glossary, including adding a definition for "activity" and incorporating the definition of "covered defense information" from DFARS 252.204-7012.

### Next Steps

While the DOD still has many hurdles to clear in the implementation of the CMMC certification process, Rev 0.7 demonstrates that the CMMC model itself is in a near-final form for the expected January 2020 release. Companies who conduct business with the DOD, or who are in the DOD supply chain, should take the opportunity of this preview of the CMMC model to begin assessing compliance with the various processes and practices set forth in the model. The discussion and clarification appendices provide a valuable tool for companies to better understand what the various practices and processes entail.

---

*Amy Conant Hoang and Erica L. Bakies are associates, and Sarah F. Burgart is a law clerk at K&L Gates LLP.*



[1] Amy Conant Hoang and Sarah Burgart, **DOD Clarifies Contractor Cybersecurity Certification Process**, Government Contracts Law360 (Nov. 14, 2019).

[2] Id. at 7.

[3] Id. at 1.

[4] Id. at 3.

[5] This statement in the narrative comports with the various practices included in the CMMC model. While the model addresses best practices for incident reporting, those practices do not contain the same specific timing requirements as DFARS 252.204-7012. The specific requirements in DFARS 252.204-7012 will remain once the CMMC is implemented, and organizations subject to the clause must satisfy both those requirements and CMMC practices at their level of certification.

[6] Generic maturity processes in Rev. 0.7 include: "establish a plan that includes [DOMAIN NAME]" (Level 2); "provide adequate resources to meet the plan for [DOMAIN NAME]" (Level 3); and "review and measure [DOMAIN NAME] activities for effectiveness" (Level 4).

[7] Rev 0.7 at 2.

[8] "Practices" are technical activities, whereas "processes" are procedures to institutionalize those practices within an organization.