DOD Clarifies Contractor Cybersecurity Certification Process

By **Amy Conant Hoang and Sarah Burgart**

Amy Conant Hoang

Sarah Burgart

On Nov. 8, the U.S. Department of Defense publicly released an updated draft of the Cybersecurity Maturity Model Certification, or CMMC, framework, Rev 0.6.[1] This draft follows a previous version released on Sept. 4 (Rev 0.4) and reflects changes made in response to feedback received by the DOD on Rev 0.4.

For those familiar with the CMMC basics, the key updates to the new version include:

- Updated cybersecurity practices within level 1 though level 3, but practices within levels 4 and level 5 will not be provided until the next public release.

- Detailed descriptions of level 1 through level 3, including what types of information a certified contractor will handle at each level, what level of process maturity is required at each level, and from which existing resources and standards the cybersecurity practices associated with the levels originate.

- Reduction from 18 to 17 domains, a set of cybersecurity categories that overlie practices described in the model (eliminating the "Cybersecurity Governance" domain).

- Updated and expanded process maturity standards for each level.

- A new guide for reading the model, including clarification that once a practice is introduced within a maturity level of the model, it applies to the listed level in addition to all higher levels (practices are cumulative).

- Significant reduction in the number of practices included within level 1 through level 3, from 242 practices in Rev 0.4 to 131 practices in Rev 0.6.

- A new appendix (Appendix B) with discussion and clarification of practices for level 1, including descriptions of best practices and examples of practices being demonstrated within a company (currently limited to level 1, with level 2 to be added at a later date).

- No information to date is provided for the submission of public comments in the new version.

CMMC Overview

CMMC is a certification framework developed by the DOD that measures a defense contractor's ability to safeguard federal contract information, or FCI, and controlled unclassified information, or CUI, handled in the performance of DOD contracts. The framework includes five levels of certification ranging from level 1 (basic cyber hygiene) to level 5 (proactive and advanced cyber practices).

Each level is made up of practices and processes that a contractor must demonstrate in order to achieve that level of certification. Certification levels will be determined through assessments from independent, third-party auditors.

After implementation of the CMMC framework, the DOD will assign a maturity certification level to individual functions of each DOD procurement. These maturity levels will be listed in requests for proposals, or RFPs, and will serve as go/no-go evaluation criteria for contractors based on the certification level they have achieved.

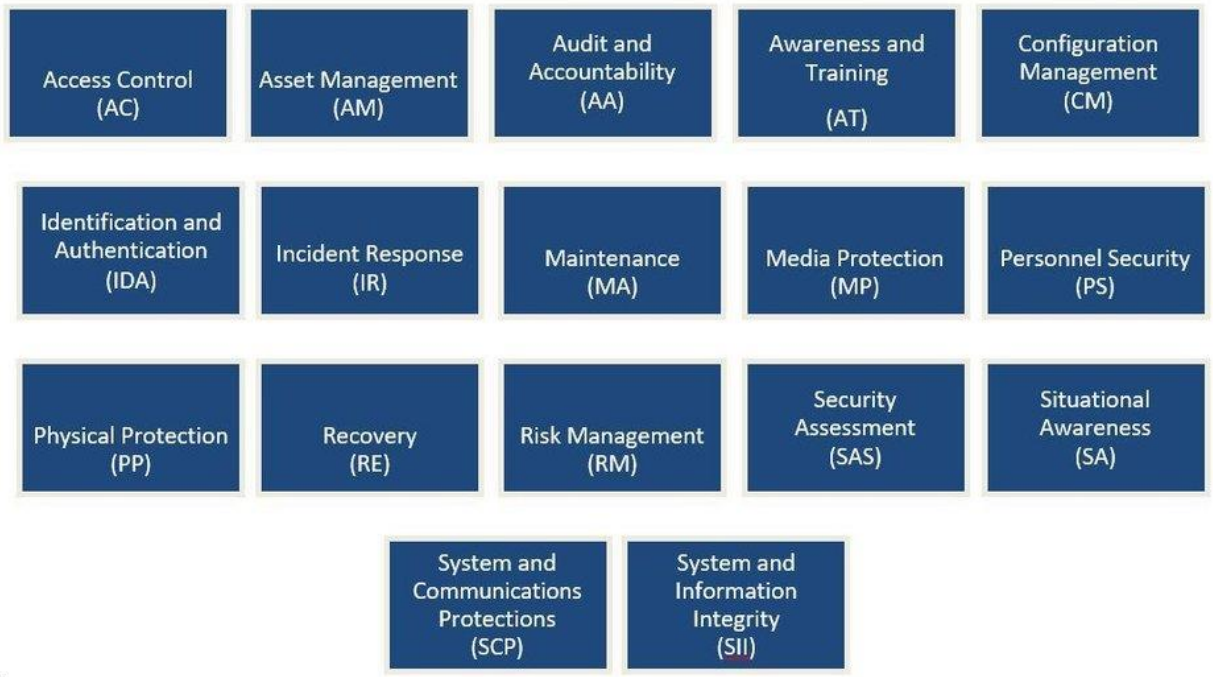
The DOD expects to release the final version of the CMMC framework in January 2020. It expects to begin including certification levels in requests for information, or RFIs, in June 2020 and in RFPs in fall 2020.

Draft Version 0.6

CMMC Framework Structure

The latest CMMC draft explains the structure of how cybersecurity best practices are organized within the framework. At the highest level, cybersecurity best practices are organized into domains, described as "[k]ey sets of capabilities for cybersecurity."

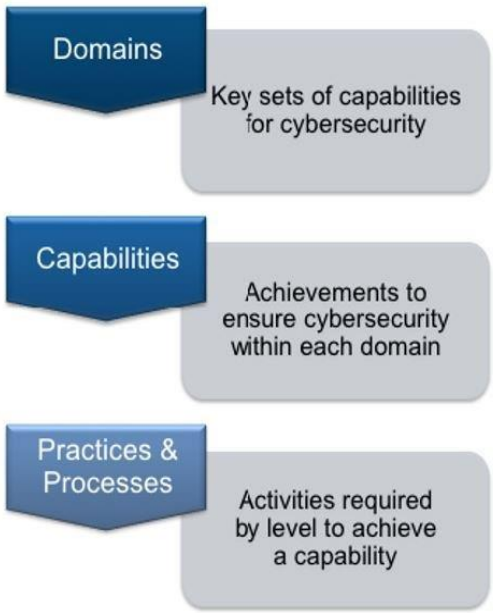
The model consists of 17 domains, the majority of which originate from the NIST SP 800-171 control families[2] and the federal information processing standards, or FIPS, 200 security-related areas.[3] The CMMC domains are:



Within each domain, the model is segmented into capabilities, described in Rev 0.6 as "achievements to ensure cybersecurity objectives are met within each domain." Within each capability, achievements are further broken down into practices and processes.

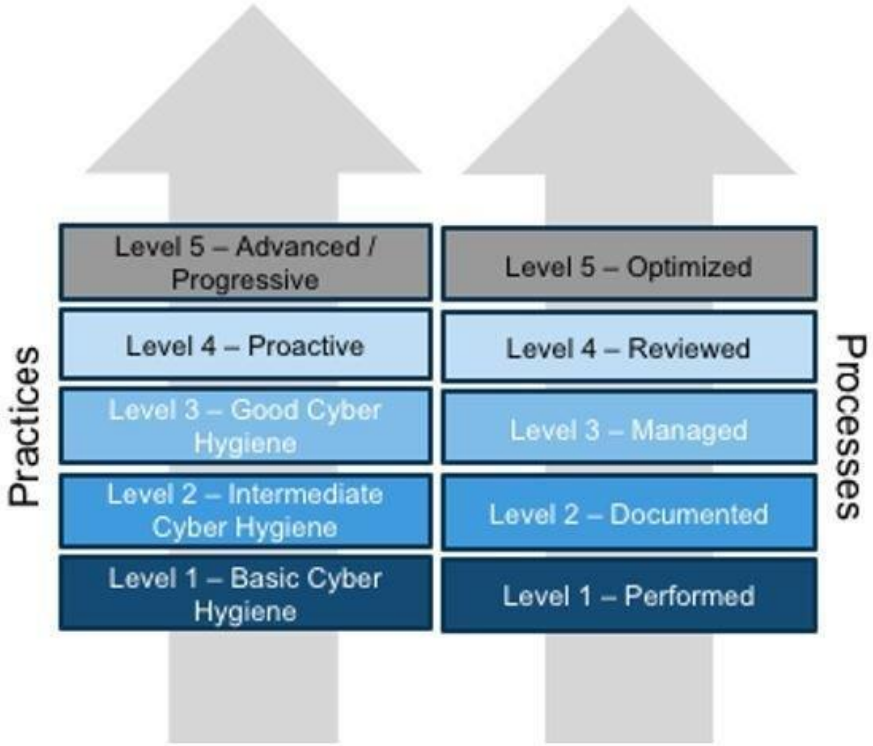
Practices evaluate technical activities that must be performed, whereas processes evaluate the extent of institutionalization of those practices within the company.

Rev 0.6 Figure 1 illustrates the relationship between domains, capabilities, and practices:



CMMC Maturity Levels

The CMMC framework includes five levels of certification, each with its own set of associated practices and processes as demonstrated in Rev 0.6 Figure 2:



In order to be certified at a specified level, a company must have achieved all the practices and processes associated with that level, as well as all levels below it.

CMMC Rev 0.6 gives an overview of each level:

- Level 1 is "a foundation for the higher levels of the model" that consists of the requirements of 48 C.F.R. 52.204-21.[4] At this level, a contractor may handle FCI not intended for public release, but it may not handle CUI. No process maturity is required at level 1, so cybersecurity practices associated with this level must merely be performed instead of institutionalized.

- Level 2 is "a maturity-based progression for organizations to step from [level] 1 to 3." Level 2 introduces the process institutionalization aspect of the model. At this level, a company must not only perform the listed practices, but it also must document standard cybersecurity operating procedures, policies and plans. A company may not yet handle CUI if it has only been given level 2 certification.

- Level 3 requires companies to have good cyber hygiene and effective implementation of controls that meet the requirements of NIST SP 800-171 Rev 1. Companies that handle or generate CUI will be required to have level 3 certification. With regard to the institutionalization of practices at this level, companies must demonstrate management of cybersecurity activities through adequate resourcing and review.

- Level 4 and level 5 require substantial and proactive cybersecurity programs, including the capability to adapt to changing tactics. Process maturity at these levels includes reviewing and measuring cyber activities for effectiveness and informing high-level management of issues at level 4, and standardizing a documented approach and sharing identified improvements across all company units at level 5.

  While the DOD did not yet provide an updated draft of the CMMC framework for level 4 or level 5, it did indicate in Rev 0.6 that some cybersecurity activities at these levels would originate from NIST SP 800-171B.[5]

Differences From Draft Version 0.4

The most significant difference between CMMC Rev 0.6 and Rev 0.4 is the size of the framework. The latest version significantly reduces the number of cybersecurity practices required in level 1 through level 3. For example, in CMMC Rev 0.4, maturity level 1 consisted of 35 separate practices that were required across 15 different domains. Rev 0.6 now includes only 17 required practices across 6 domains.

Similarly, level 2 in Rev 0.4 consisted of 115 required practices across 18 domains, while level 2 in Rev 0.6 consists of 58 required practices across 15 domains; and level 3 in Rev 0.4 consisted of 92 required practices across 16 domains, while level 3 in Rev 0.6 consists of 56 required practices across 16 domains. Overall, Rev 0.6 significantly reduced the size of the model previously provided in Rev 0.4.

Another difference between the two versions is the latest version's inclusion of a discussion and clarification for level 1 practices. For each of the 17 practices associated with maturity level 1, CMMC Rev 0.6 Appendix B includes a discussion of the practice and a clarifying explanation that includes one or more examples of how the practice could be demonstrated within a company. While the new version only includes discussion and clarification for practices associated with level 1, it also says that the final version released in January will include clarification for level 1 and level 2.

Looking Forward

Unlike CMMC Rev 0.4, the latest version of the CMMC framework (at least as of this publication date) does not call for public comments on the draft model of level 1 through level 3. Instead, stakeholders may have to wait until the DOD releases the draft model for levels 4 and level 5 to provide further input.

The DOD still expects to publish the final version of the full CMMC framework in January

2020. With that in mind, companies that do business with the DOD (even those further down in the supply chain) must start preparing for implementation:

- Review the practices provided in Rev 0.6 and start assessing where you company stands. Pay particular attention to practices in Level 3, which the DOD has indicated it expects the majority of contractors to achieve.

- Consider whether the CMMC audit process provides an opportunity for your company to participate as a Third-Party Assessment Organization (still in early stages of development).

- Begin to assess whether your supply chain will be able to meet the various levels, as the DOD has indicated that the CMMC will apply to lower-tier subcontractors as well as primes.

- For companies anticipating procurements that may be assigned level 4 or level 5, continue to monitor for updates to the level 4 and level 5 practices, which the DOD has indicated will be released in the next update.

Amy Conant Hoang is an associate and Sarah F. Burgart is a law clerk at K&L Gates LLP.

[1] https://www.acq.osd.mil/cmmc/docs/CMMC-V0.6b-20191107.pdf.

[2] NIST Special Publication (SP) 800-171 Revision (Rev) 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, U.S. Department of Commerce National Institute of Standards and Technology (NIST), December 2016 (updated June 2018), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[3] FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, U.S. Department of Commerce, March 2006, available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[4] 48 C.F.R. 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

[5] NIST SP 800-171B, DRAFT Protecting Controlled Unclassified Information in Nonfederal

Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets, U.S. Department of Commerce NIST, June 2019, available at https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf.