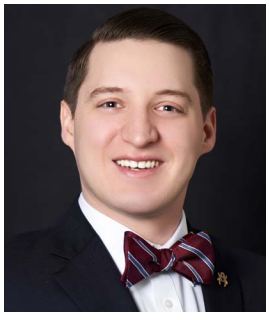
ARTICLE

U.S. Department of Defense Institutes New Cybersecurity Maturity Model Certification

Published in American Bar Association Forum on Construction Law Division 13 Newsletter, Volume 5, Issue 2, Spring 2020



JOSEPH N. FROST

For More Information Please Contact

Joseph N. Frost
jfrost@pecklaw.com
202.293.8815

Contractors doing business with the Federal Government, particularly with the Department of Defense ("DoD"), commonly handle sensitive information that is not intended to be disseminated. Controlled Unclassified Information ("CUI") is one such type and is more specifically defined as "information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations and government-wide policies."[1] Because some DoD contracts require contractors to handle CUI, certain safeguards have been put in place to ensure its security. This article briefly touches on the current cybersecurity protocols, followed by a discussion of the new system being developed by the DoD, and what contractors most need to know about the new system.

The Defense Federal Acquisition Regulation Supplement ("DFARS") has long required contractors to comply with certain cybersecurity standards, as published by the National Institute of Standards and Technology ("NIST"). Specifically, DFARS sought to implement the cybersecurity framework found in NIST Special Publication ("SP") 800-171, entitled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST SP 800-171 sets forth fourteen (14) families of recommended security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations, including, among others, access control, audit and accountability, incident response, personnel security, and system and information integrity. However, after a series of data breaches, the DoD reassessed the efficacy of the continued use of NIST SP 800-171 and ultimately decided to institute a new methodology to ensure the security of CUI.

Basics of the Cybersecurity Maturity Model Certification

The DoD, after consultation with prominent DoD stakeholders, University Affiliated Research Centers, Federally Funded Research and Development Centers, and the Defense Industrial Base sector, has promulgated the Cybersecurity Maturity Model Certification ("CMMC"). The CMMC is a certification program designed to gauge an organization's proficiency at protecting CUI. In addition, the CMMC seeks to protect Federal Contract Information ("FCI"), a category of less-sensitive information that is provided by, or generated for, the Government under contract and is not intended for public release.

The CMMC is new, with some portions still under consideration. Version 1.0 was released in January 2020. An updated Version 1.02 was released in mid-March with administrative changes, keeping intact the substance of Version 1.0. The DoD initially expected to begin incorporating the CMMC requirements in its Solicitations starting in June 2020, but has not issued a statement on what, if any, effect the COVID-19 pandemic has had on the implementation. However, it is likely the implementation will be delayed. The DoD has plainly stated that every Solicitation will eventually require a specified

minimum CMMC level, and plans a phased implementation resulting in all contracts incorporating the CMMC by sometime in 2026. Contractors unable to meet the CMMC requirements will be automatically ineligible for that contract.

To protect CUI and FCI, the CMMC "measures an organization's cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats."[2] To do so, the CMMC incorporates best practices from multiple cybersecurity standards, frameworks, and other references, including but not limited to those from NIST Special Publications, International Organization for Standardization, and Aerospace Industries Association.

The Five CMMC Maturity Levels

Under the framework of the CMMC, there are five maturity levels through which an organization's cybersecurity is measured. The description of the levels as they pertain to processes, starting at the lowest level (Level 1), are: Performed; Documented; Managed; Reviewed; and Optimizing. The descriptions of the levels as they relate to practices, also starting at Level 1, are: Basic Cyber Hygiene; Intermediate Cyber Hygiene; Good Cyber Hygiene; Proactive; and Advanced/Progressing. The requirements for each level are cumulative, meaning that for an organization to obtain a particular level of certification, it must also demonstrate that it has satisfied all of the processes and practices required for the lower levels. If an organization achieves different levels with respect to the processes and practices, the organization will be certified at the lower of the two levels.

The level that a contractor should seek will depend on the work it is looking to perform for the DoD. The Solicitation will specify the minimum required CMMC level. The higher the level at which an organization is certified shows an increased ability of that organization to protect CUI and FCI. The levels of CMMC each have a particular focus:

- Level 1 – Basic Safeguarding of FCI
- Level 2 – Serves as Transition Step in Cybersecurity Maturity Progression to Protect CUI
- Level 3 – Increasing Protection of CUI
- Levels 4-5 – Protection of CUI and Reducing the Risk of Advanced Persistent Threats

This framework of levels, processes, and practices is designed to measure an organization's cybersecurity proficiency within seventeen (17) domains, many of which were drawn from NIST SP 800-171. Domains represent different areas of concern. Within each domain are particular categories of processes and capabilities that an organization must undertake. There are specific required practices associated with each domain depending upon the Level. The Domains are: (1) Access Control; (2) Asset Management; (3) Audit and Accountability; (4) Awareness and Training; (5) Configuration Management; (6) Identification and Authentication; (7) Incident Response; (8) Maintenance; (9) Media Protection; (10) Personnel Security; (11) Physical Protection; (12) Recovery; (13) Risk Management; (14) Security Assessment; (15) Situational Awareness; (16) System and Communications Protection; and (17) System and Information Integrity.

Each of the five levels consists of delineated *processes* and *practices*. In the context of the CMMC, processes are plans that an organization has put in place regarding cybersecurity and related systems. Through the CMMC, an organization's process institutionalization can be measured. That is, the CMMC can determine the extent to which plans are embedded into an organization. The more deeply ingrained an organization's processes are, the better that organization will be able to protect CUI. The CMMC consists of five processes that span Levels 2-5, and are applicable to all domains. Because it is possible organizations may only perform Level 1 practices in an ad-hoc manner and may not keep documentation, the CMMC does not assess process maturity at Level 1.

The five CMMC processes are as follows:

Level 2
(1) Establish a policy that includes [DOMAIN NAME], and
(2) Document the CMMC practices to implement the [DOMAIN NAME] policy

Level 3
(3) Establish, maintain, and resource a plan that includes [DOMAIN NAME]

Level 4
(4) Review and measure [DOMAIN NAME] activities for effectiveness

Level 5
(5) Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units

Whereas *processes* measure the institutionalization of an organization's plans, *practices* are the specific actions an organization can utilize to implement cybersecurity protocols. There are 17 practices at Level 1; 55 at Level 2; 58 at Level 3; 26 at Level 4; and 15 at Level 5. As previously discussed, the levels are cumulative in nature, so to achieve a Level 2 certification a contractor must meet 72 total practices. In total, there are 171 practices across the five levels, split among the various domains. Some examples of CMMC practices, taken from different domains and levels, are: Verify and control/limit connections to and use of external information systems; Monitor and control remote access sessions; Ensure equipment removed for off-site maintenance is sanitized of any CUI; Protect and monitor the physical facility and support infrastructure for organizational systems; and Utilize sandboxing to detect or block potentially malicious email.[3]

A helpful summary is provided by the CMMC itself: "The Cybersecurity Maturity Model Certification ('CMMC') framework contains five maturity processes and 171 cybersecurity best practices progressing across five maturity levels. The CMMC maturity processes institutionalize cybersecurity activities to ensure they are consistent, repeatable, and of high quality. The CMMC practices provide a range of mitigation across the levels..."[4]

What Contractors Need to Know About the Cybersecurity Maturity Model Certification

While the framework of the CMMC has been thoroughly fleshed out, there are still some compliance and certification requirements that remain to be announced by the DoD. This section will cover the key points of which a DoD contractor should be aware.

1. *Implementation of CMMC*

The DoD originally planned to begin including CMMC requirements in selected Requests for Information ("RFI") in June 2020 and in selected Solicitations in the Fall of 2020. The COVID-19 pandemic as well as the delay in issuing the proposed DFARS rule implementing CMMC will likely delay this initial implementation phase. The DoD expects all contracts to incorporate the CMMC requirements by 2026. As of now, the use of CMMC is confined to the DoD, though other agencies and departments may adopt its use in the future.

2. *Certification*

When implemented, CMMC certification to the required level will be a Go/No Go decision. A prospective bidder or offeror must be certified at or above the required CMMC level to be eligible for award. Self-certification will not be allowed. Instead, contractors will be certified by accredited, independent, third-party commercial certification organizations known as CMMC Third Party Assessment Organizations ("C3PAOs"). As of the writing of this article, no C3PAOs have yet been accredited, meaning there are not yet any credentialed C3PAOs able to conduct a CMMC assessment. As C3PAOs become accredited, the CMMC-Accreditation Body will publish a list of accredited C3PAOs. The contractor will be able to specify the desired CMMC level at which it would like to be certified and will be awarded certification dependent upon a showing of satisfactory maturity in the processes and practices required for that level. A contractor's certification level will be made public, but details regarding specific findings will not be publicly available. Certifications are expected to be valid for three years.

3. *Cost of Certification*

As of now, the cost for certification has not been determined. However, it is likely that the cost will increase as the desired CMMC level increases. The DoD has stated, however, that the cost of certification will be considered an allowable, reimbursable cost and will not be prohibitive. In other words, the cost of certification should be an allowable cost. Whether the contractor can direct charge the cost, or must include the cost in its overhead, is unclear and will likely vary depending upon the contractor's accounting system and the type of contract. However, except for cost-reimbursement contracts, it is unlikely that the contractor will be able to bill the DoD directly. Additionally, while the DoD has stated the cost of certification will be reimbursable, it is likely that cost of becoming compliant will not be directly reimbursable.

4. *Who Must Be Certified?*

While the DoD initially advised that every contractor who does business with the DoD must be certified, the DoD more recently advised that commercial off-the-shelf ("COTS") suppliers will not have to be CMMC certified. With the exception of COTS suppliers, the requirement to obtain a CMMC certification flows down to subcontractors and suppliers at all tiers, although subcontractors may not be required to be certified to the same level as the prime contractor. If your organization does not handle CUI, then it is likely you will only need to be certified at Level 1. However, if your organization does handle CUI, then you will need to be certified to Level 3 or higher.

Conclusion

The CMMC synthesizes various cybersecurity protocols into a single framework created specifically to protect sensitive DoD information. Adding the certification element allows the DoD to easily verify that a particular contractor has put the necessary protocols in place to safeguard CUI, thereby lessening the risk of disclosure of sensitive information.

More information can be found by visiting the following URL: www.acq.osd.mil/cmmc

---

[1] Exec. Order No. 13556, 75 C.F.R. 68675 (2010).

[2] Under Sec'y of Def. for Acquisition and Sustainment, Dep't of Def., Cybersecurity Maturity Model Certification, at 1 (Ver. 1.02) (2020).

[3] Under Sec'y of Def. for Acquisition and Sustainment, Dep't of Def., Cybersecurity Maturity Model Certification, at 12-22 (Ver. 1.02) (2020).

[4] Under Sec'y of Def. for Acquisition and Sustainment, Dep't of Def., Cybersecurity Maturity Model Certification, at 23 (Ver. 1.02) (2020).

Published in American Bar Association Forum on Construction Law Division 13 Newsletter, Volume 5, Issue 2, Spring 2020.