Armstrong Teasdale

July 31, 2020 • Publications • www.atllp.com

STAYING COMPETITIVE: ADDRESSING CMMC RISKS BEFORE IT'S TOO LATE

NCMS Bulletin

By Brian Kaveney, Colleen Kinsey and Thomas Langer

PEOPLE

Brian E. Kaveney

Colleen Kinsey

These days, it is easy to get bogged down with information relating to COVID-19. However, there is one topic on the horizon that contractors must keep a close eye on and educate their leadership about. CMMC, or the Cybersecurity Maturity Model Certification, is a topic we all must watch closely and consider its future impact for compliance and revenue. There is a great deal of information packed into CMMC, but three important issues stand out and require education of functional areas within your organization. Under CMMC, all defense contractors will be **required** to be certified at the relevant level for cybersecurity compliance in order to obtain Department of Defense (DOD) contracts.

The first issue is "Certified Third-Party Assessment Organizations" and what happens when these assessors begin gaging the systems of contractors. CMMC changes the requirement that contractors certify the security of their IT systems by now requiring third-party assessments of contractors' compliance with certain *mandatory* practices, procedures and capabilities.[1] All DOD contractors must participate in accreditation and satisfy the requirements of Level 1 at a minimum.[2]

Level 1: Basic Cybersecurity Hygiene: Contractors should implement cybersecurity measures that are considered common practice, such as antivirus software and periodic password updates. These practices should be equivalent with Federal Acquisition Regulation (FAR) 48 CFR 52.204-21.

Level 2: Intermediate Cyber Hygiene: This level includes universally accepted cybersecurity best practices that must be documented. This level requires multi-factor authentication to protect Controlled Unclassified Information (CUI).

Level 3: Good Cyber Hygiene: Contracts must implement additional practices beyond the minimum scope of current CUI protection. This includes all practices from NIST SP 800-171 r1.

Level 4: Proactive: This level includes advanced and sophisticated cybersecurity

practices. The processes at this level should be periodically reviewed, properly resourced and regularly improved to proactively maintain compliance.

Level 5: Advanced / Progressive: This is the highest level, and the security measures in place should encompass Levels 1-4, as well as highly advanced cybersecurity practices. The processes involved at this level include continuous improvement across the enterprise and defensive responses performed at machine speed. Contractors should have additional enhanced practices that provide more sophisticated capabilities to detect and respond to Advanced Persistent Threats (APTs).[3]

Levels and requirements are subject to change as cybersecurity threats and protections are developed.

The National Institute of Standards and Technology (NIST) will assist in developing the specific standards and accreditation process. Notably, CMMC Levels 1-3 include NIST security requirements to protect CUI.[4] If contractors are not proactive in evaluating their systems to meet the requirements of the CMMC levels appropriate for their contract, they will ***likely*** fall behind when assessors begin gaging the systems. Contractors wishing to be among the first to receive accreditation had to meet requirements *as early as* June 2020. The CMMC Accreditation Body has begun accepting applications for those wishing to be certified third-party assessors to be accepted and participate in training prior to assessments taking place. Early preparation will **help** contractors transition when accreditation begins.

*Second, what is the process for an appeal or due process if an audit goes poorly?*In our view, there is nothing worse than not having a remedy after a poor result. One of the most significant concerns for contractors of **all** sizes is what type of due process will be available if a certification level or audit result is *erroneous.* The CMMC assessments could have a **significant impact** on contractors' ability to meet *minimum*contract requirements, and a low rating could limit a contractor's ability to meaningfully compete for work. A poor result is often difficult to explain to management . . . Currently, the CMMC does not establish a contractor's right of appeal, although DOD indicates it is coming. Given these factors, it is important for functional areas such as IT, contracts, legal and security to work together, communicate and plan for the assessment. As with any assessment from the U.S. Government, these functional areas must prepare for a myriad of results and ensure they properly educate their leadership about the resources needed to plan and prepare, particularly during this dynamic environment. Perhaps, this will result in leaders providing more resources given the lack of due process to help ensure compliance with the requisite CMMC level of accreditation.

Third, how will CMMC accreditation impact contractor liability under the False Claims Act (FCA)? The federal government indicated, in two cases, that it would

prosecute claims brought under the FCA for failure to comply with applicable cybersecurity measures.[5] Prior to the implementation of the CMMC, government contractors were tasked with evaluating their own compliance with government cybersecurity standards.

In *Aeroject*, defendants misrepresented cybersecurity compliance to government officials.[6] This case made clear that cybersecurity compliance is a material aspect of contracts where there is a standard or necessary adequate protections for data.[7]

The new CMMC accreditation poses an interesting question regarding contractor liability: when a third-party assessor conducts the accreditation and assigns the requisite level, who can face liability under the FCA? The contractors will be relying on the trained third-party assessment of their cybersecurity protections. This may offer some protection under FCA, although it is unlikely there will be a decrease in the number of FCA claims related to cybersecurity.

In July 2019, CISCO reached a settlement in a whistleblower action under the FCA alleging the company did not have proper cybersecurity measures in place. [8] The $8.6 million settlement, while CISCO did not admit any wrongdoing, may suggest that the *possibility of a cyber breach* is sufficient to form the basis of FCA liability.

It is doubtful that FCA claims brought in cybersecurity will decline. It is unclear, however, whether the third-party assessors will be liable under the FCA for misclassifying the contractor's compliance with cybersecurity. With CMMC implementation beginning in 2020, this new accreditation process may provide some relief for contractors worried about violating the FCA, since the process will be carried out by third-party assessors. However, contractors will be required to maintain their systems to ensure continued compliance with their applicative level of accreditation or face liability under the FCA to avoid exposing data to the possibility of a breach.

CMMC implementation is moving forward, and contractors vying for DOD contracts must increase their cybersecurity measures with meaningful policies that conform to the necessary level of accreditation. Contractors should document all changes and improvements. Finally, leaders ranging from program managers to security must work together, understand the required certification, evaluate whether the appropriate resources are assigned, and raise CMMC awareness across their environment to prevent rogue networks. This approach will prevent a poor result and enable contractors to win business while protecting the appropriate information.

Originally published in the NCMS Bulletin. Reprinted with permission.

[1] Office of the Under Secretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification FAQs,* https://www.acq.osd.mil/cmmc/faq.html (last visited 4 July 2020).

[2] *Id.*

[3] Carnegie Mellon University & The Johns Hopkins University Applied Physics Laboratory, Cybersecurity Maturity Model Certification (2020), https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf (last visited 6 July 2020); C. Todd Lopez, *DOD to Require Cybersecurity Certification in Some Contract Bids,* U.S Dept. of Defense, https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/ (last visited 6 July 2020); Abigail Stokes & Marcus Childress, *The Cybersecurity Maturity Model Certification Explained: What Defense Contractors Need to Know,* CSO, https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html (last visited 6 July 2020).

[4] *Maturity Model Certification FAQs, supra* note 1.

[5] *U.S. v. Aerojet Rocketdyne Holdings, Inc.,* 381 F. Supp. 3d 1240, 1246 (E.D. Cal. 2019); *U.S. v. Cisco Systems*, Case No. 1:11-cv-400 (W.D.N.Y. May 5, 2011).

[6] *Aerojet*, 381 F. Supp. 3d at 1246.

[7] *Id.*

[8] See Stipulation of Dismissal (ECF No. 75), No. 1:11-cv-00400-RJA (W.D.N.Y., filed May 10, 2011).