PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

DGC
ACCOUNTING • TAX • ADVISORY
A DIVISION OF PKF O'CONNOR DAVIES, LLP

Major Updates to the Cybersecurity Maturity Model Certification

By Scott Goodwin, Manager, IT Risk Assurance and Advisory

The United States Department of Defense (DoD) views securing the supply chain and defense industrial base (DIB) as one critical pillar in protecting national security. Dedicated security requirements exist for the protection of federal information systems and classified information, based on the NIST 800-53 standard. However, several years ago, a gap was identified in the security requirements applied and enforced for the protection of non-federal systems and controlled unclassified information (CUI). The steps initially taken by the DoD to enhance supply chain security ended up having significant implications for nearly all organizations that do work with the DoD.

Past Security Methods

In a nutshell, the DoD began requiring organizations that handle CUI to comply with the 110 security requirements outlined in NIST 800-171 via the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. This contractual obligation required defense contractors to "self-attest" their compliance with this standard, as well as maintain a System Security Plan (SSP) and Plan of Action and Milestones (PoAM) to document security gaps.

The Cybersecurity Maturity Model Certification (CMMC) was developed to address some of the shortcomings of this original approach. It was determined that while the security standard itself (NIST 800-171) was appropriate, the DFARS clause had no "teeth"—that is, no accountability. The self-attestation model and broad allowance for non-compliant items (i.e., PoAMs) meant that many defense contractors did not *actually* implement the standard, manage their security program or remediate non-compliant items. CMMC sought to fix these issues by moving to an independent third-party certification model, enhancing the framework with five different levels of security maturity, removing the allowances for PoAM items and introducing significant documentation and governance requirements by means of "process maturity" requirements.

Proposed New Security Requirements

Fast forward to today—past the initial DFARS rule, past the initial self-attest implementation of NIST 800-171 requirements and past the idealistic vision introduced with CMMC version 1.0, the DoD has again revised the requirements for security compliance within the DIB with CMMC version 2.0. In many ways, CMMC 2.0 represents a "back to basics" approach by removing certain components of the original model that were deemed unnecessary or overly burdensome for the defense supply chain. The following represent the major revisions within CMMC 2.0:

- Version 2.0 reduces the number of maturity levels from five to three, removing the CMMC version 1.0 levels two and four. Organizations that process controlled unclassified information will now find themselves pursuing CMMC 2.0 Level 2 compliance, compared with Level 3 compliance in CMMC version 1.0.

- The additional 20 technical requirements (the "delta 20") added in the evolution from NIST SP 800-171 to CMMC version 1.0 Level 3 are eliminated, meaning the requirement for organizations within the DIB that process CUI is back to the NIST 800-171 standard.

- All process maturity requirements which were net-new with CMMC version 1.0 have been eliminated.

- CMMC 2.0 Level 1, for organizations that process federal contract information, remains mostly unchanged except that an annual self-assessment now suffices for government compliance, rather than certification by a CMMC 3rd Party Assessment Organization (C3PAO).

- CMMC 2.0 Level 2 requires the implementation of NIST SP 800-171. Some contracts with Level 2 requirements will require triennial certifications by a C3PAO. Other contracts will be satisfied by an annual self-assessment. The criteria which determine the contracts pegged for C3PAOs vs self-assessment are unknown at this time.

- CMMC 2.0 Level 3 largely equates to the previous Levels 4 and 5 and will require the implementation of NIST SP 800-172. Only a government-led assessment team can certify an organization to Level 3 and not a C3PAO.

- Plan of Action and Milestones are back on the table. Previously, an organization seeking certification (OSC) needed to implement 100% of the requirements to be certified. Under CMMC 2.0, OSCs may be certified with some number of open items. Certain requirements must be implemented for certification and contract award, and some PoAMs will be allowed as long as the plan to implement has a clearly identified timeline. The guidance around the allowances for PoAM items has not yet been clarified.

Effective Date

The changes reflected in CMMC version 2.0 will be implemented through the government rulemaking process in Part 32 of the Code of Federal Regulations and in the Defense Federal Acquisition Regulation Supplement (DFARS). This means that the rulemaking process may not be finalized for another nine to 24 months, meaning it will be some time before organizations begin seeing CMMC version 2.0 as a contractual obligation.

Proceed Under Existing Contract

What should you do now? The DoD has indicated it does not intend to approve the inclusion of a CMMC version 2.0 requirement in any contract prior to the completion of the CMMC 2.0 rulemaking process. However, most companies planning for CMMC compliance are already subject to FAR 52.204-21 and/or DFARS 252.204-7012, which require the implementation of certain technical safeguards. These existing contractual obligations remain unchanged and largely form the basis of the CMMC 2.0 Levels 1 and 3 respectively. Therefore, companies should continue to build and maintain compliance programs and close PoAM items pursuant to their contractually obligated compliance frameworks.

Contact Us

If you have questions related to these defense industrial base compliance requirements or other steps you can take to assess and secure your environment, contact your engagement team or either of the following:

Scott Goodwin
Manager
IT Risk Assurance and Advisory
sgoodwin@pkfod.com

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
IT Risk Assurance and Advisory
ndelena@pkfod.com

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.