Updates
June 25, 2020
DoD’s Cybersecurity Verification Regime: New Details Emerge Related to Third-Party Auditor Training and Accreditation

A key area of focus in the Department of Defense's (DoD) gradual rollout of its Cybersecurity Maturity Model Certification (CMMC) is the training and accreditation of third-party assessors that will be responsible for reviewing some 300,000 defense contractors' cybersecurity practices for compliance with applicable controls.

On June 22, 2020, the CMMC Accreditation Body (CMMC-AB), the newly created non-governmental entity managing various aspects of CMMC, announced new details on its website outlining how entities can become certified to perform third-party assessments under CMMC. According to the CMMC-AB's website, certified training will begin in "Winter 2020/21," and commercial assessments under CMMC will be available starting in "Winter/Spring 2021."

This update provides an overview of the latest developments related to CMMC, including plans to train and accredit auditors, and their significance for contractors preparing for CMMC.

CMMC and Third-Party Verification

CMMC establishes a unified cybersecurity framework to protect government information in the possession of defense contractors against cyber threats. The program reflects DoD's focus on protecting so-called Controlled Unclassified Information in DoD's supply chain from malicious cyber activity as a matter of both national and economic security.

CMMC is being introduced into new DoD contracts through 2026, starting with an initial slate of "pathfinder" contracts this year. Ultimately, every defense contractor (except for commercial off-the-shelf suppliers) will need to obtain a certification from a neutral third party known as a Third-Party Assessment Organization, or C3PAO.

In order to become CMMC certified, a contractor must have the capabilities, processes, and practices required under DoD's CMMC model, which establishes five levels of controls ranging from Level 1 (basic hygiene) to Level 5 (Advanced/Progressive). The CMMC model framework organizes processes and cybersecurity best practices into a set of 17 capability "domains." Contractors will be required to be certified at the time of award of a DoD contract.

CMMC's creation of a third-party verification regime raises new compliance issues and costs for contractors. It is a significant departure from the existing regulatory framework for protecting "defense covered information" set forth in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. As implemented by DoD, that clause essentially relies on contractors self-attesting their compliance with cybersecurity controls set forth in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171.

Latest Developments

Since DoD released Version 1.0 of its CMMC model in January 2020, several initiatives have laid the groundwork for its gradual implementation across DoD's supply chain.

On March 23, 2020, the CMMC-AB signed a Memorandum of Understanding with DoD outlining the roles, responsibilities, and authorities of DoD and the CMMC-AB. DoD announced on June 1, 2020, that it is also finalizing a "zero cost" contract with the CMMC-AB.

DoD is also planning to issue requests for information associated with its "pathfinder" contracts sometime this summer. DoD is also engaged in a rulemaking process to revise its cybersecurity clause in DFARS 252.204-7012 to implement CMMC. The degree to which the COVID-19 crisis disturbs the rulemaking timeline remains to be seen. The prospect of forthcoming regulatory changes based on comments from the public creates uncertainty in the program.

New Details Related to Training and Credentialing of Third-Party Assessors

The CMMC-AB's latest announcement focuses on establishing a "provisional program" for the credentialing and training of C3PAOs and credentialed individuals, including Certified Assessors that will conduct assessments. On May 27, 2020, the CMMC-AB issued requests for information to obtain market research related to training and delivery of exams for applicants.

DoD will only accept certifications under CMMC from an assessor or a C3PAO that has been accredited for assessments by the CMMC-AB. No qualified CMMC assessors presently exist, so training and accreditation are necessary to create a workforce from scratch. According to the CMMC-AB's website, its accreditation "ecosystem" will "go live" in "Winter/Spring 2021."

According to CMMC-AB's revised website, the CMMC-AB is now accepting applications from interested entities and individuals seeking accreditation in various roles. Entities seeking to become a certified C3PAO must pay application and annual fees and be subject to an organizational background check. They will also have to sign a license agreement and code of professional conduct. C3PAOs must be 100%-owned by U.S. citizens, but the website says that foreign ownership is "under exploration for all C3PAOs." Individuals seeking to become Certified Assessors must complete a training program and pass an examination and background investigation. There is also a designation—Registered Practitioner—for those seeking to provide consulting services to companies related to CMMC without performing the formal assessments.

An Assessment Process That Could Take Six Months

The CMMC-AB's updated website also sheds light on the requirements for companies to become CMMC certified. According to a timeline on the CMMC-AB website, the certification process could take "6 months (or more)" with several steps:

- Contractors seeking certification under CMMC must first identify what CMMC Maturity Level they need to obtain among the five CMMC levels. Companies possessing Controlled Unclassified Information will have to be certified at least at Level 3.
- Contractors will next schedule a CMMC assessment by identifying a C3PAO using the CMMC-AB's "marketplace" portal. The extent to which contractors will be able to essentially shop for a C3PAO (and what criteria may be used to do so) remain unclear. According to the CMMC-AB's website, it plans to publish a list of available assessors after the training is complete and assessors have been certified.
- According to the CMMC-AB, C3PAOs are authorized to enter into contracts with companies seeking certification. As discussed below, this raises several questions.
- C3PAOs will schedule an assessment of the contractor to be carried out by a Certified Assessor.
- Once the third-party assessor has performed an assessment of the company's systems against the CMMC model, the CMMC-AB's Quality Auditors will review the assessment. They will have up to 90 days to resolve any findings with the C3PAO.
- If the contractor's system is deemed to satisfy the requirements in the CMMC model for the appropriate CMMC Level, a CMMC Maturity Level certification will be issued, thus enabling the contractor to bid on and obtain DoD contracts subject to that CMMC level.
- The CMMC certificate obtained by the contractor will be valid for three years.

Takeaways

CMMC is still in the early stages of its rollout. Proper training and accreditation of the C3PAOs and individual assessors are obviously critical given their role in the program and the sheer scale of the effort spanning the entire Defense Industrial Base. Quality control, uniformity, and predictability will be important aspects of any successful implementation of the model.

The latest information released by the CMMC-AB highlights several issues that will no doubt continue to be discussed and considered.

- The CMMC-AB's reference to CMMC-AB Quality Auditors reviewing C3PAO assessments raises several questions. What standard will those Quality Auditors use when conducting their reviews? How long will take it? How searching (or how deferential) will a Quality Auditor be of a C3PAO's individual assessment?
- According to the CMMC-AB's website, contractors seeking certification will enter into contracts with C3PAOs. This relationship raises several questions. For example, what terms will apply? Which source of law will govern? How will disputes be governed? To what extent will there be uniformity in such contracts across the CMMC program?
- The cost impact of CMMC for small businesses is a recurring concern, especially given the economic fallout from the COVID-19 crisis. There is also ongoing uncertainty as to how CMMC will be applied and flowed-down to lower-tier subcontractors.
- Another area is conflicts of interest. DoD has indicated that C3PAOs should not be allowed to essentially audit their own company. But questions remain about the details.

Companies preparing for CMMC should continue to monitor announcements from DoD and the CMMC-AB and consider what steps they can take now to prepare. The DFARS rulemaking will be especially important because it will provide clarity on the requirements for industry.

Authors

Explore more in

Privacy & Security Government Contracts

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law