ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

JULY 19, 2021

Department of Defense's CMMC: Where Is It Now?

by Amy Mushahwar, Jon Knight, and Kim Peretti

Whether it is actors, musicians, sports stars, or just general celebrities from a bygone era, people are always interested in a "where are they now" story. And even though it is a little less exciting than discovering that Vanilla Ice now hosts a home remodeling TV show, the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) has consistently made headlines as it has evolved and changed since was first announced in early 2019.

Intended to be a unifying standard for the implementation of cybersecurity across the defense industrial base (DIB), the CMMC's requirements are already being felt even though the program is not yet fully operational. For example, as of November 30, 2020, all government contractors with a DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, clause in their contracts were required to conduct a self-assessment of NIST SP 800-171 standards and enter their results into the Supplier Performance Risk System (SPRS). COVID-19 and other challenges arose in 2020, resulting in delay to the program and critical delays in staffing assessors. Despite these delays, some DoD contracts moved forward with CMMC pilot programs in 2021, such as the Space Force, which added such requirements to a broadband global area network request for information.

There are strong indications that other civilian agencies are also evaluating the CMMC. For example, the General Services Administration's (GSA) $50 billion STARS III solicitation, a government-wide RFP for IT services from qualifying small business primes, includes a reference stating that "[w]hile CMMC is currently a DoD requirement, it may also have utility as a baseline for civilian acquisitions; so it is vital that contractors wishing to do business on 8(a) STARS III monitor, prepare for and participate in acquiring CMMC certification." Federal contractors at all levels should keep an eye on the status of the CMMC rollout because satisfying the requirements will take time, it has the potential to impact most DoD procurements, and we can expect to see similar requirements rolling out to other agencies (as indicated by the GSA reference and in the recent Executive Order from the Biden Administration on Improving the Nation's Cybersecurity).

CMMC: What Is It and Does It Apply to Me?

Dozens of articles have already been written explaining the nuts and bolts of the CMMC, but a brief reminder is always helpful. The CMMC is a cybersecurity maturity certification program divided into five levels of processes and practices: (1) basic cyber-hygiene; (2) intermediate cyber-hygiene; (3) good cyber-hygiene; (4) proactive; and

(5) advanced/progressive. These levels, achieved based on scoring for up to 173 different controls, are derived from multiple other cybersecurity standards but unified into a whole framework. The DoD intends the levels to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes—ranging from basic cyber-hygiene to robust "zero trust" network controls—are in place for protecting certain information that resides on the department's industry partners' networks.

The CMMC has a very broad reach. While it will not apply to acquisitions of purely commercial-off-the-shelf (COTS) items, it will apply to all other DoD solicitations and contracts valued at greater than the micro-purchase threshold ($10,000). Importantly, contract awards will be conditioned on certification for the required CMMC level, and the certification requirements will flow down to all tiers of subcontractors (based on the sensitivity of the information that flows down to the subcontractor). In other words, the CMMC is not just for large defense contractors or for procurements of weapons systems. It will ultimately touch all levels of the DIB.

Contractors Cannot Be Certified Until Assessors Are Accredited

In order to be certified at a particular CMMC level, a contractor must be assessed by a CMMC Third-Party Assessment Organization (C3PAO). As of May 2021, there had been 100+ C3PAOs cleared by the CMMC Accreditation Board to be assessed and approved, but only two had completed the assessment process to be conducted by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and appear on the CMMC Accreditation Body Marketplace. Until C3PAOs are available, contractors cannot be assessed and certified under the CMMC. However, the DIBCAC has announced that it is performing C3PAO assessments throughout the summer, and we can expect these newly certified assessors to be available to conduct contractor assessments shortly thereafter. Contractors are encouraged to monitor the FAQs and other announcements on the CMMC Accreditation Body website for the latest information.

Provisional Period Assessments?

In the interim, 101 individuals have been selected as provisional assessors (PAs) from the individual assessor applicant pool and appear on the CMMCAB Marketplace. Their role, as experienced cybersecurity professionals, is to provide feedback on the assessment guide and methodology. They are not fully accredited assessors, and they are not permitted to certify a company's compliance until they are fully accredited. Instead, PAs may conduct CMMC provisional assessments for readiness of an organization. PA status is provisional and remains valid through six months after formal certified training is available. During this period, PAs are expected to transition from the provisional status to a certified assessor by taking the applicable courses and exams. Even if contractors cannot schedule one of the two authorized C3PAOs, those eager to begin the process and understand how their security program appears to an auditor may at least begin these provisional-period gap assessments.

While the Timeframe to Include CMMC Requirements in DoD Contracts Has Slipped, the Deadline for Self-Attestation of Certain Controls Has Not

Originally, the DoD anticipated that requests for information and solicitations would start to reference CMMC requirements beginning in the summer of 2020, but the formal pilots started much later in 2021.

While full CMMC certification levels may not yet be contractually required unless a contractor is participating in a CMMC pilot, an interim self-attestation requirement is now in effect for the DoD agencies. Per DFARS 252.204-7019, if a prime or sub is required to implement NIST SP 800-171, then it is now required to conduct a self-assessment under NIST SP 800-171 and upload the assessment score to SPRS "in order to be considered for [contract] award." This

requirement went live in November 2020. If you have already provided your assessment score to the SPRS, there is no need update it in the near future. The assessment must be "current," meaning "not more than 3 years old unless a lesser time is specified in the solicitation." However, if you have not yet performed the assessment and uploaded the score, you cannot receive an award. During the April 2021 CMMC town hall, the DIBCAC director indicated that at least some contractors have had delays in receiving their awards because they waited until too close to the award deadline to pursue this assessment.

The DoD's Approval Process for C3PAOs Illustrates What Will Likely Be Expected for Contractors Once Assessments Begin

During the April 2021 CMMC town hall, hosted by the DOD-authorized CMMC Accreditation Body, DIBCAC Director Darren King shared the DIBCAC's assessment timeline for approving C3PAOs and indicated contractors seeking a Level 3 CMMC certification should expect a similar process to what is required to become a C3PAO. He also provided advice on pitfalls in the certification process so far based on what they are seeing when approving the C3PAOs.

Overall, contractors can expect a six-week assessment timeline for a Level 3 certification. However, this is an ambitious timeline and assumes a significant amount of work by the contractor before beginning the assessment process. Four weeks before the assessment, the contractor should expect pre-coordination meetings to go over the types of documentation that will be needed for the assessment. For example, a contractor can expect to be asked for a system security plan, relevant policies and procedures, a customer responsibility matrix for all cloud or hosted services, and a documentation traceability matrix. Then, two weeks before the assessment, contractors can expect a readiness review. Essentially, this will be a pre-read of the relevant documentation to ensure that time is not being wasted by assessing an organization that is clearly not ready for a Level 3 assessment. One week before the assessment, the contractor can expect to finalize the interview and demonstration schedule, and the contractor can expect the assessment itself to take approximately one week. The post-assessment work (finalizing the reports and memoranda) is currently expected to take one to two weeks.

King emphasized that contractors need to be well-prepared *before* starting the assessment process and identified several potential pitfalls:

> *Assessment pitfall: open items on a plan of action and milestones (POAM)*. This has potential to trip up contractors because open POAM items are currently allowed when attesting to NIST SP 800-171. However, they are not allowed for CMMC certification, and a contractor should not begin the assessment process with any open items.
>
> *Assessment pitfall: cloud confusion*. King noted many contractors do not have a clear understanding of cloud responsibility. This lack of understanding is reflected in unclear policies and procedures around the use of cloud technology. Contractors without a clear, accurate matrix of cloud responsibility are not, in King's view, ready for a CMMC Level 3 assessment.
>
> *Assessment pitfall: incomplete or draft policies and procedures*. Whether the system security plan or other relevant policies and procedures, King cautioned against relying on draft or incomplete documentation. He recommended focusing on making sure the policies are internally consistent and that no placeholder language remains because these are clear red flags that a contractor is not ready for the assessment process.

Assessment pitfall: neglecting to conduct a self-assessment before starting the process. Starting the assessment process without first having conducted a self-assessment is like going to take a test without having studied even though you were given the answer key. All contractors will have access to the CMMC Assessors Guide, and King strongly encouraged conducting a self-assessment using the guide before beginning the assessment process. A rigorous self-assessment will identify potential gaps and provide contractors with the opportunity to address those gaps. This self-assessment is particularly important during the early phases of the CMMC rollout because there will be a limited number of assessors and time for completing the assessments.

We also now have insights from the few C3PAOs that have passed their DIBCAC assessment. During the June 2021 CMMC town hall, a representative from RedSpin shared lessons learned from the assessment process that will apply to contractors seeking certification under the program.

Certification will need company-wide engagement, not just participation from IT or infosec. Every policy and process needs an owner, and the questions will touch on many aspects of the business outside the IT/infosec arena. For example, you may need a person who can explain or certify how your company knows it is budgeting enough for IT/infosec. You may need someone to speak to your recruiting processes and how you know your organization is targeting people with the correct skill set to support your CMMC certification and ongoing compliance. Contractors should expect the certification process to involve stakeholders from across the company, including the CFO, director of human resources, and others—not just your CIO or CISO.

Work now to narrow the scope of what needs to be certified. The RedSpin representative emphasized the need to know what and who touches your controlled unclassified information (CUI). Then, before you start the certification process, take a hard look at whether you can narrow this scope. For example, is there ever a need to have CUI accessed via a mobile device? If not, put controls in place to make sure that your mobile devices and associated policies and procedures are out of scope for the certification.

Please stay tuned to our blog for further updates regarding the CMMC as this program evolves with the DoD (and likely other civilian agencies).

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our **publications subscription form**.

Learn more about our **Privacy, Cyber & Data Strategy Team**.

Learn more about our **National Security & Digital Crimes Team**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Co-leaders of the National Security & Digital Crimes Team

Kellen Dwyer
202.239.3240
kellen.dwyer@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Amy S. Mushahwar
202.239.3791
amy.mushahwar@alston.com

Jon Knight
202.239.3270
jon.knight@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333