Getting Started with CMMC: How to Prepare and What to Expect from the Assessment

Related People:
Alexander W. Major

Cybersecurity Law Report

02.03.2021

Growing concerns around supply chain threats have led to the DoD's increased regulatory focus on strengthening and securing the federal supply chain with the Cybersecurity Maturity Model Certification (CMMC) framework. Current and prospective contractors should be preparing now for compliance with the framework, which requires a third-party cybersecurity audit and certification by 2025 (earlier for some) as a prerequisite to doing business with the DoD.

Also touting the value in conducting a "self-assessment to get an understanding of where the company thinks it is," McCarter & English partner Alexander Major opined that companies in the Level 3 or 4 space should enlist a vendor "to come out and just kind of check their math." While he recommends that all companies at Levels 3 and 4 (explained in more detail in part one) should seek third-party assistance, he noted that many companies, especially small- to medium-sized ones, face the challenge of having a very savvy IT department, but not necessarily a very savvy IS department. "That can become problematic if the IT department says it implements certain controls but there is no one to push back on that, or double check the systems." In those instances, it is helpful to have a third party come in to check that the necessary controls and procedures are in place, he advised.

For companies that have not been part of the government contractor space yet, a very basic starting point for getting into the space would be to "meet the requirements of NIST SP 800-171, and ensure that the company is scoring above 100 in the DFAR 7020 assessments. That should be where the company is targeting," advised Major.

Major cautioned, however, that "a lot of companies tend to view NIST SP 800-171 as a race that starts at mile 0, but it's actually a race that starts at mile 10." NIST SP 800-171 is built on assumptions, set forth in the appendix, that companies already have an incident response plan and other policies and procedures in place, he explained. What many contractors also may not realize, he pointed out, is that NIST SP 800-171 addresses confidentiality, "but to have robust cybersecurity you also need to make sure that your data integrity and data availability is protected." NIST SP 800-171, for example, does not contain a requirement for companies to back up their data. It only requires that if a company does back up its data that it also secures it.

CMMC Levels 1 and 2 build in the NIST SP 800-171 assumptions, requiring companies have those plans, policies and procedures in place before they get to Level 3, Major noted. Levels 1 and 2 not only require data safeguards, but also necessitate steps to back up data, protect access to it, and ensure that if it is altered, it can revert back. “That is a benefit of CMMC – it fleshes out robust cybersecurity, not just the safeguarding component,” he opined.

Many of the companies that already have a contract with the DoD with a DFARS 7012 clause likely qualify or are close to qualifying for Level 3 certification, Major suggested. They should examine the CMMC standards and create an assessment to see what additional steps they will need to take, which is basically the equivalent of a POA&M (plan of action and milestone), to satisfy the additional 18 elements of Level 3. Likely, they “will just have to fill in some of the blanks on the NIST SP 800-171 appendix assumptions that they might not have operationalized.”

From a business practicality standpoint, companies also should “examine what is inherent in Level 4 that makes sense and is within reach,” because, Major predicted, “there’s going to be a lot of fallout due to the SolarWinds breach,” and that may prompt DoD to “require the enhanced security requirements of NIST 800-171B, which will be found in CMMC Level 4,” for companies that are “working on high-profile or novel weapon systems, or are tangentially connected to operational missions.” Those companies could find their current DFARS 7012 contract including a Level 4 or higher requirement and should “definitely begin prepping or understanding the path from Level 3 to Level 4, and then maybe start doing cost estimates for what that will entail,” he suggested.

Given the time that compliance can take, companies should start down that path now and not rely on the fact that certification is required at the time of the award and not when the proposal is submitted, Major advised. Putting a proposal together is also expensive, he noted, so a company does not want to find itself in a position where it put together a proposal for a job it cannot fulfill because it is not at Level 4 and it cannot be certified at Level 4 for another six months. “Generally, you may not know when these draft RFPs are going to come out with a Level 4 requirement but when they do, you want to be in a position to say you can meet those requirements,” he stressed.