DLA PIPER

DoD’s new cybersecurity compliance program . . . What you need to know

Government Affairs Alert

6 November 2019
By: Dawn E. Stern

The Department of Defense (DoD) is actively developing a new framework for protecting government data and evaluating contractors’ cybersecurity compliance, known as the Cybersecurity Maturity Model Certification program (CMMC). With the impending finalization of the CMMC framework, here is the “who, what, when, where, why and how” that you need to know:

- **Who?** The CMMC requirements will apply to all DoD contractors and subcontractors. In other words, all contractors that perform under a contract that contains a CMMC requirement will be required to be certified under the program. However, it is not yet clear how the requirements will flow down the supply chain. Further, while the current CMMC model will apply only to DoD contracts, it is expected that a certification model will be developed for civilian agencies. However, the civilian agency model likely will look very different from CMMC, taking into account the wide range of missions and types of data that exist across agencies.
- **What?** Unlike the existing DFARS requirements, the CMMC framework is expected to have five levels of potential compliance, ranging from a basic cybersecurity program (Level 1) to sophisticated practices for the most advanced contractors (Level 5). The existing DFARS requirements (*i.e.,* compliance with the NIST SP 800-171 controls) are expected to equate to Level 3. The level required for contract performance will be determined on a contract-by-contract basis. Importantly, contractors and subcontractors will no longer be permitted to self-certify compliance. Under the new

model, contractors must obtain a third-party assessment by a company that has been accredited as an official CMMC Third-Party Assessment Organization.
- **When?** DoD has released and sought comments on draft versions of the program and expects to release its next draft early this month. DoD's goal is to publish the final version of the model in January 2020, with the CMMC requirements to start appearing in RFIs and solicitations during the summer and fall of 2020.
- **Where?** Once incorporated into the procurement process, the CMMC will allow DoD to establish a requisite certification level for each contract. The required certification level will be set out in solicitations, and only contractors who have received the requisite level certification or higher will be eligible for award. However, contractors will not be required to obtain contract-specific certifications. This means that contractors are not required to get recertified each time a bid is submitted. However, it will be important for contractors to anticipate the certification level commensurate with the cybersecurity maturity required for the type of work the company performs.
- **Why?** DoD believes that the current system is not working to adequately protect Government data. "We're losing," Katie Arrington, Special Assistant to the Assistant Secretary of Defense, said when explaining current cybersecurity threats. Compromises in cybersecurity systems currently cost the United States $600 billion per year, and DoD expects that number to increase rapidly if changes aren't made soon. Additionally, US adversaries are targeting smaller companies and companies that do not have access to classified information because their cybersecurity systems are more lax. Hackers are targeting the weak links in our systems to obtain massive amounts of data that, even if unclassified, can disclose sensitive information. DoD hopes to close this loophole by setting a floor for cybersecurity with all of their contractors.
- **How?** It is not yet clear how long obtaining a certification will take or how much it will cost. DoD hopes to keep costs of certification low and plans to make such costs allowable in order to ease the burden on businesses. However, while the cost of obtaining the certification may be allowable, it's not clear that the business costs of revamping current cybersecurity measures in order to obtain the certification will be. Businesses can expect that these costs may be significant, depending on the level of certification they hope to obtain. Additionally, a certification won't last forever. It is still up in the air how long a certification will remain in effect before recertification is necessary. Katie Arrington has voiced some preference for a relatively short shelf life, but DoD has not officially endorsed this. It is also unclear how the Government will keep up with the demand for assessments.

We anticipate that there will be a relatively tight turnaround for comments when the next version of the model is released for comment. Accordingly, organizations should start considering now whether they would like to comment and what issues they may want to address in those comments. Providing comments is an excellent way to raise concerns with DoD in advance of the CMMC's formal release.

AUTHORS

Dawn E. Stern
Partner
Washington, DC | T: +1 202 799 4000
dawn.stern@dlapiper.com