Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

DOD Cybersecurity Rollout May Be Delayed By COVID-19

By **Daniel Wilson**

Law360 (May 22, 2020, 6:30 PM EDT) -- The U.S. Department of Defense still has much to finalize within its sweeping new cybersecurity program for defense contractors, and COVID-19-related restrictions mean its timeline for rolling out the new plan may be too ambitious.

First announced in May 2019, the Cybersecurity Maturity Model Certification, or CMMC, will require all defense contractors to get a cybersecurity level rating from one to five, with minimum required ratings eventually attached to all future defense contracts. The DOD has said it expects roughly 300,000 contractors and suppliers will need to be certified over time.

As the coronavirus pandemic rages on, the DOD has kept in place its plan to include CMMC requirements in several contract requests for information — an early information-gathering stage of procurement — in June as part of a pilot program. Its anticipated date to start including cyber requirements in some contract requests for proposal, or RFPs, has recently slipped from September to November.

But with all the parts that need to be put in place to implement such a sweeping change to cybersecurity requirements, including new rules and a network of compliance assessors, the constraints caused by the pandemic may make even that extended timeline unrealistic, said K&L Gates LLP partner David Yang.

"I think it's going to slip beyond November because of the fact that DOD's current plan — and I think it's appropriate — is that they want to put new requirements into the [Defense Federal Acquisition Regulation Supplement]," he said. "If there is a delay, which I think is more likely than not, then I can see the RFPs get pushed into the following year."

DOD Special Assistant for Cybersecurity Katie Arrington, one of the key officials in charge of the CMMC rollout, has said those RFPs will not be released until there is a related DFARS rule formally implementing the CMMC.

She has also said that the department will not issue that DFARS rule until it has a chance to hold a public meeting and gather industry feedback. Although Arrington said at a conference May 11 that she expects the rule to be completed by October, it is unclear when the underlying meeting will happen, given social distancing restrictions.

"I don't know that it's going to occur within the next 30 days, or the next 60 days, and I think that's going to delay things if they continue to say they have to have a public meeting before they finalize the rule," Stinson LLP partner Susan Warshaw Ebner said.

Although the DOD could ultimately change its mind and try to conduct its initial CMMC implementation through alternative means such as a class deviation or an interim rule, that would go against its current efforts, which have involved a lot of industry outreach. CMMC is also a major change to contracting and it would be problematic to not have a public comment period, according to Ebner.

"The real benefits of having a public meeting is that people have an opportunity to raise issues that DOD may not be thinking of," she said. "That frequently happens during the notice-and-comment period — industry is able to identify the practical aspects of, 'You want this to happen, but maybe the way you've established this procedure may not work.'"

Even after a meeting, the DOD will need time to formulate a proposed rule, which will then be open for additional feedback before a final rule is crafted, a step which often takes months on its own, and which could be further complicated if COVID-19 comes roaring back once restrictions are lifted, leading to a second round of shelter-in-place requirements.

Once there is a final rule, contractors will also need time to finalize their CMMC implementation plans and prepare for related audits to determine their CMMC level.

"CMMC is not going to be a situation where people can just flip a switch and — bam! — we're [meeting] CMMC," said Alex Major, co-chair of McCarter & English LLP's government contracts group.

Although the DOD has a CMMC "Version 1.02" plan in place and is also releasing additional information over time through webinars, panels and other public forums, lack of formal final guidance means contractors are effectively "horseshoe and hand-grenading" their efforts to meet CMMC requirements, hoping they are close to the standards they will need to meet, Major said.

"I recognize the litany that the policy folks keep saying about the risk and the threat and the challenge and the need [for cybersecurity] and I think contractors all recognize that, and now they're just waiting. 'What would you like us to do about it?,'" Major said. "'We're trying to meet you, but we don't want to walk down this path only to find out [we need to go another way].'"

One of the biggest open questions is how much Level 3 of CMMC will diverge from requirements in the National Institute of Standards and Technology's Special Publication 800-171, a high-profile existing cybersecurity standard that the DOD had previously said Level 3 would hew closely to.

There is also the issue of the lack of a standard federal definition for "controlled unclassified information," which is important for contractors to understand exactly what information they need to protect and therefore what CMMC level they need to shoot for.

Also important — and outside the DOD's direct control — is how companies will be certified to meet a particular CMMC level. The DOD has outsourced assessments to an independent accreditation body, which in turn will accredit third-party auditors.

The board's training committee chairman, Ben Tchoubineh, said in a May 21 webinar that the board is still waiting on the DOD to finalize a training course for auditors, and that it expects a first class of 60

potential CMMC auditors to begin training this summer.

That first phase of the training program, a precursor to a more formal training program scheduled to begin in 2021, should be finished within three to six months, and although Tchoubineh said that initial training is intended to meet the DOD's deadline for the first CMMC RFPs, that may be cutting it close.

The picture of what the DOD expects from contractors could become clearer after the initial requests for information that include CMMC requirements go out in June, which could effectively serve as a "beta test," providing key data for further refinements, said Covington & Burling LLP partner Susan Cassidy.

"There is always a benefit to beta testing," she said. "And I'm sure industry is not going to be shy about raising concerns or issues, with an eye towards making it a better process."

It is important for the DOD to ultimately get the program right, as other federal agencies are looking at CMMC as a potential model for their own cybersecurity programs, according to Cassidy.

"If this works … if it's a decent process, it would be a better process than what we have now," she said. "When a client asks me what are the cybersecurity requirements if I want to become a government contractor, it's like, 'Which agency do you want to work with?'"

--Editing by Kelly Duncan and Emily Kokoll.
