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

Audit Process Remains A Mystery In DOD Cybersecurity Plan

By **Daniel Wilson**

Law360 (February 5, 2020, 8:33 PM EST) -- The Pentagon's new cybersecurity requirements for defense contractors are raising concerns about how those standards will be implemented, with details missing on how contractors can get audited and certified.

While the U.S. Department of Defense heeded comments to ease up on its initial aggressive implementation timeline and clarify requirements for subcontractors, it remained silent on key parts of the certification process for contractors when it released its final Cybersecurity Maturity Model Certification, or CMMC, last week.

Questions about the process, such as who will audit the thousands of contractors that need to be certified for cybersecurity compliance, how they will be audited and what options they will have if they disagree with an audit, remain unanswered, said Susan Cassidy, a Covington & Burling LLP partner whose practice focuses especially on defense acquisition issues.

"This is the 'devil is in the details' part of it, in many ways the hardest part of this, because it's the practical implementation [of the plan]," she said. "And I'm hoping [the DOD] ... seeks industry input, because industry will think of practical issues that they may not have, because they're not on the business side of it."

The CMMC will eventually require all defense contractors to get a cybersecurity level rating from one to five, and will attach minimum ratings to future defense contracts. The DOD has said it expects roughly 300,000 contractors and suppliers will need to be certified, and plans to put that certification process in the hands of a nonprofit oversight body, which will approve third-party auditors.

"The accreditation process still seems like it's the long pole of the tent," Cassidy said. "The concern there, and I don't know if they've thought about this [although] I'm assuming they have, is what are the qualifications to be an accreditor ... and how are they going to vet that? Because you're going to have what appears to be a lot of smaller entities — it doesn't mean they're not good, but my guess is it'll be uneven. So how are they going to ensure quality?"

Being able to challenge a certified CMMC level will be a crucial requirement for contractors, which will be barred from bidding on contracts if they don't meet the minimum required level, according to Miles & Stockbridge PC principal Cameron Hamrick, who has tracked the progress of the CMMC throughout its various drafts.

"Because it's an all-or-nothing proposition ... you can bet that contractors are going to be fairly aggressive about considering their legal options," he said.

If there is no clear avenue for appeal, contractors could be "stuck" with their CMMC level for as long as three years, which is how long a certification will last, Cassidy said.

"We need some due process in there," she said.

The DOD's cybersecurity model also leaves contractors in the dark about whether they will have an auditor assigned or get to choose their own. It is also unknown how much sensitive information companies will need to provide to get certified and how auditors and the DOD will protect that information, Hamrick said.

"Obviously, DOD is going to take whatever steps it can to ensure that this data is, to the greatest extent possible, protected, but DOD — just like contractors — has experienced repeated attacks that increase in sophistication, and so ... contractors are going to be a little hesitant to provide that information," he said.

David Yang, an Oles Morrison Rinker & Baker LLP partner, said that contractors should begin the certification process as soon as possible to ensure eligibility for future contracts since it is unknown how long an audit could take and there could be a considerable audit backlog.

"Everyone's being advised that you really need to act now," Yang said.

The DOD's responsiveness to industry input so far while developing the CMMC raises hopes that the department will adequately resolve the outstanding concerns with the certification and audit process, Cassidy said.

Through various drafts of the plan, the department slashed requirements and beefed up associated guidance that will be especially welcomed by smaller companies and nontraditional defense contractors, McCarter & English LLP's government contracts practice co-chair Alexander Major said.

"Some can look at it, especially the more advanced contractors, and see it as somewhat patronizing, but I think that's actually super helpful — baby step me through the process, don't make assumptions on what I'm doing if you're not actually telling me what to do," said Major, who focuses a significant part of his practice on cybersecurity requirements in federal procurement.

The latest version of the CMMC also responds to earlier concerns that the timeline for the rollout would

be too aggressive, saying that it will use a "crawl-walk-run" process that will take until 2026 to fully implement, as well as clarifying that cybersecurity requirements for prime contractors won't necessarily carry through to subcontractors on the same contract.

Instead, the required cybersecurity level for subcontractors will depend on what information has been shared from prime contractors, DOD Special Assistant for Cybersecurity Katie Arrington said Jan. 31, an announcement that helps alleviate concerns about the plan's impact, especially on small businesses.

While more details are needed on who will be responsible for determining the type and amount of information that needs to be shared, including whether it's the prime contractor or the DOD, and what is considered protected or sensitive information, Arrington's clarification was still "heartening," Hamrick said.

"It shows DOD's understanding of the need to be flexible in certain areas," he said.

--Editing by Breda Lund.