Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Big Shift Unlikely In Cybersecurity Regs, Despite Concerns

By **Daniel Wilson**

Law360 (March 8, 2024, 12:55 PM EST) -- The U.S. Department of Defense is unlikely to significantly alter its cybersecurity proposals for contractors, despite calls from its private industry base for more flexibility and clarity.

The DOD received nearly 800 comments from contractors, trade groups and others in response to the rule it proposed in December to implement the sweeping Cybersecurity Maturity Model Certification program, which sets out expanded cybersecurity requirements for contractors and their third-party providers.

Common concerns include murkiness around when and how the DOD will adopt changes to third-party cybersecurity standards, and which contractors will be able to self-assess their cybersecurity programs.

But according to attorneys who have been closely watching the DOD's rulemaking process on the CMMC and other cybersecurity rules, the final CMMC rule is unlikely to depart significantly from the proposal. The department already had to scrap an earlier interim version that contractors said was too complicated and rigid; it pushed forward to include some requirements in the proposed rule despite earlier complaints; and it refused to extend its deadline for comment submissions, all suggesting an eagerness to hedge closely to what it already has on paper and to finalize its proposal sooner rather than later.

"I read some comments that were very, very thoughtful ... and yet, they're suggesting strategic or structural changes in the rule that amount, either individually or cumulatively, to a reset," said Bob Metzger, co-chair of Rogers Joseph O'Donnell PC's cybersecurity and privacy practice group, who helped draft several industry comments on the rule. "And DOD isn't going to do that. They are going to look at what they've proposed and look for things to clarify. I think the bar will be fairly high to persuade them to make a change."

The DOD is legally obligated to consider all relevant comments on proposed rules, but it is not required to adapt suggestions into the final versions. The department did not respond to questions on its current planned timeline for finalizing the CMMC rule and its response to comments on the proposed rule.

The first proposed version of the CMMC program was set out in a 2020 interim rule, but complaints from contractors spurred the department to issue a draft "Version 2.0" in November 2021.

That draft formed the basis for the December proposed rule, and has already been subject to extensive

industry feedback addressing many of the same concerns raised in recent comments, showing the department was already aware of those concerns but pushed ahead with the bulk of its draft plans anyway, said Jeff Chiow, co-chair of Greenberg Traurig LLP's government contracts practice.

"Many of those issues were raised before, they were dealt with in some detail in the rule, and I expect that there will be minor adjustments rather than wholesale changes in any of those areas," he said.

The DOD also rejected requests to extend its comment period despite explicit requests from stakeholders, sticking with its original 60-day deadline when it frequently grants similar requests "in these more intense kinds of cybersecurity rulemaking," Hogan Lovells partner Stacy Hadeka said. That is likely a signal that it wants the rule finalized without delays, further slimming hopes for significant changes, Hadeka said.

"Maybe they are going to be comfortable that it's OK to not get it perfect [to begin with], and then maybe there will need to be additional updates down the road or some class deviations that might need to get issued in order to address items that come up throughout the whole implementation period," she said.

The DOD may also have a vested interest in wanting to finalize the rule before a new Congress and a potential new president may decide to review it early next year, according to Metzger.

"My thought is that the DOD is seeking to finish this, if they can, sometime in early to mid-October, so that the rule can be finalized with 60 days remaining before the end of the present congressional session," Metzger said.

The parts of the rule where the DOD is most likely open to making changes are where those changes will alleviate implementation issues, not only for the companies subject to CMMC but for the department itself, attorneys said.

For example, the DOD said in its proposed rule that it anticipates the vast majority of the roughly 76,500 contractors that will fall under Level 2, the middle tier of CMMC requirements, to require a third-party assessment rather than being able to self-assess their compliance with CMMC.

But the department also wants to roll out CMMC across all defense contractors and subcontractors within two and a half years of finalizing the rule, and there may not be enough third-party assessors available to conduct assessments of tens of thousands of companies within that timeline, said Crowell & Moring LLP counsel Michael Gruden, a registered CMMC practitioner.

"When we keep going exponentially further and further out, extending these compliance requirements, it does come to a point of — Is this tenable for the contracting community? Is this tenable for the [CMMC Third Party Assessment Organization] community?" he said. "We may see the DOD take a risk-based approach, perhaps defining the scope of those requirements more finitely in the final rule."

The DOD may also be more open to making material changes to sections of the proposed rules that hadn't previously been announced, such as clarifying the line between managed-service providers, or MSPs — third-party information technology providers for contractors — that use certain cloud-based services, and those considered to be cloud-service providers, or CSPs.

Under the proposed rule, MSPs that handle controlled unclassified information are subject to the same

cybersecurity standards as contractors under CMMC. But CSPs are expected to get authorization under more stringent standards adopted from the National Institute of Standards and Technology.

The proposal is unclear on whether MSPs that use cloud services as a peripheral part of their business would be subject to the more stringent cybersecurity standards, and imposing those higher standards on them could be "devastating to the industry," Chiow said.

"It's one thing to expect [MSPs] to meet [CMMC] requirements, I think it's a logical and rational decision," he said. "But it's not simple. And taking that next leap ... if that's the DOD's intention, which I suspect that it's not — that's the kind of thing that really is a departure from what anyone expects from this very long process of how we got here, and I think it does deserve some good treatment in the rule."

Given the DOD's potential reluctance to make significant changes to the proposed rule, contractors and their third-party providers will likely need to prepare to comply with the rule largely as proposed, according to Chiow.

"I do think a lot of the wishful thinking that there will be major changes or major relaxation of the requirements is probably wasted effort, and not helpful," he said. "There's a real national security reason for these requirements, and we should be figuring out how to get it done right, not questioning whether we should do it."

--Editing by Daniel King.
