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's Haste May Spell Turbulent Start For Cybersecurity Plan

By **Daniel Wilson**

Law360 (October 24, 2019, 10:59 PM EDT) -- The Pentagon's aggressive timeline for overhauling cybersecurity requirements for defense contractors and a lack of clarity in how it expects contractors to meet those standards could make for a rocky rollout or lead to delays.

The U.S. Department of Defense's goal for its Cybersecurity Maturity Model Certification, or CMMC, program, is to improve cybersecurity by creating minimum requirements for defense contracts and a unified standard across its supply chain.

While contractors generally welcome a modernized and unified cybersecurity model to replace the current patchwork of requirements, details of the CMMC plan — set to be finalized by January — were sparse at its initial rollout in May, leaving contractors and industry groups wanting for information.

Although the DOD has released more information since May and a draft "Version 0.4" plan in September, there are still unanswered questions and issues that need clarification ahead of the final plan, said McCarter & English LLP's Alexander Major, who focuses a significant part of his practice on cybersecurity requirements in federal procurement.

"The mad dash to get it done on an important yet still artificial deadline is probably going to cause a lot of stress in the contracting community and [defense industrial base] community," he said.

For example, of the five cybersecurity levels that the DOD intends to assign to its contractors — from level 1 to level 5, the most stringent requirement — it said that level 3 would be the closest to the National Institute of Standards and Technology's Special Publication 800-171, a set of existing cybersecurity standards, Major said.

Many defense contractors are familiar with SP 800-171, since its requirements have already been incorporated into defense acquisition regulations, and attorneys have long advised their government contractor clients to aim for compliance with those requirements, Major noted.

But the requirements to be certified at level 3 outlined in the DOD's 0.4 draft don't always follow the language in SP 800-171, and the requirements in the NIST publication have been split between CMMC certification levels in ways that don't entirely make sense, Major said.

Differences between the first three cybersecurity levels, which will be the most common — levels 4 and

5 are intended only for certain critical defense programs — are particularly murky, according to both Major and Oles Morrison Rinker & Baker LLP partner David Yang.

And the amount of DOD acquisitions that will likely fall under each level is also unclear, which limits contractors' ability to decide how to tailor their cybersecurity programs, Yang said.

“Without having some kind of market study as to the percentage of procurements that are going to fall within each of the various levels, it’s going to be hard for industry to say, ‘OK, we don’t need to spend the money and resources to get compliant with levels 3, 4 and 5, because 80% of the work we’re going to be pursuing is going to be on level 1 and 2,'” Yang said.

Another area of uncertainty is whether the minimum cybersecurity level that will be rolled into defense contracts must be met not only by a prime contractor but also its subcontractors, or by every member in a teaming arrangement, where two or more companies team up to submit a joint bid on a contract.

Such teaming arrangements are already complicated and can take years to put together for big defense procurements, said Covington & Burling LLP’s Susan Cassidy, whose practice has a strong emphasis on defense acquisition issues.

And although the DOD has said cybersecurity compliance will be considered an allowable cost for defense contractors, not all contractors have cost-basis contracts, Cassidy noted. Commercial suppliers in particular often sell through fixed-price deals and may decide the burden of doing business with the DOD no longer makes sense, she said.

And that is just the tip of the iceberg for the uncertainty around the plan, according to Cassidy, who said that although the defense industry understands the overall concept, she could “probably come up with 20 questions” that the DOD has left open in the 0.4 draft.

“The overall point is that the devil is in the details here,” she said.

That ongoing uncertainty is shown in the high volume of comments received on the 0.4 plan — more than 2,000, the DOD’s acquisition chief, Ellen Lord, said in a press conference earlier in October.

The heavy volume of comments wasn't a surprise to Yang or Cassidy, the latter of whom pointed to the “sea change” inherent in the CMMC, but Major and Todd Overman, Bass Berry & Sims PLC’s government contracts practice chair, found it to be unusual. Major noted that the 0.4 draft plan was not opened to comments through the Federal Register, and was only open for comment for a short time.

The DOD’s next draft plan, Version 0.6, is due in November, and a clear comparison between the requirements in SP 800-171 and similar CMMC requirements would be welcome in that draft, as would clearer identification of what the CMMC plan requires that isn’t currently addressed by the NIST standards, Major said.

“Really, what contractors have been told for the past seven years is look to NIST,” Major said. “So how these compare to NIST — I think that is what contractors need to see.”

The DOD also should make sure minimum cybersecurity levels are included in contracts as pass-fail threshold requirements, rather than as subjective assessments that open up new grounds for bid protests, Overman suggested.

A set of clear requirements for contractors to meet is particularly important given the DOD's timeline — variously described as aggressive or ambitious — with Version 1.0 of CMMC currently scheduled to be released in January and minimum rating requirements set to be included in DOD solicitations from fall 2020.

With that deadline only months away, most attorneys Law360 spoke to suggested they expect the DOD will push back its timeline for implementing the plan.

Previous changes of a similar magnitude to the CMMC often took significant time for contractors to implement and required adjustments from the DOD along the way, Cassidy noted.

"I never want to say they can't do something, but I hope what they do is, if they need to delay a reasonable amount of time to get a better result, that they do that," she said.

And the DOD will have to deal with the "immense" logistical challenge of certifying an estimated 300,000 contractors and suppliers, as well as recruiting the third-party auditors it intends to use for those certifications, Thompson Hine LLP counsel Joseph Berger said.

But the Pentagon only recently put out a call for nonprofits to express their interest in acting as an oversight body to certify those auditors, and it will take time for a nonprofit to be selected and then do its job — a process that could be delayed if any related contract is protested, Overman said.

"Think about the volume of contractors that will be required to go through this third-party assessment, or audit — whatever you want to call it," he said. "That's just a lot of companies. So it's a little concerning … as to how we're going to be in a place a year from now where this has not become a barrier to entry."

--Editing by Aaron Pelc and Alanna Weissman.