LAW360

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

Assessment Draft For DOD Cyber Program Lacks Key Details

By **Daniel Wilson**

Law360 (August 5, 2022, 9:44 PM EDT) -- A recent draft assessment plan for the U.S. Department of Defense's pending cybersecurity program lacks important details necessary for contractors to make sure they're fully on the right track ahead of a formal rule expected next year, experts said.

The DOD plans to implement its Cybersecurity Maturity Model Certification program to address what it has said are "increasingly frequent and complex cyberattacks" against the defense industrial base. The draft assessment process released in late July sets out a proposed process for third-party assessors to review certain contractors' CMMC compliance.

That plan from the CMMC Accreditation Body, or Cyber AB, is aimed mostly at those assessors, known as C3PAOs, for CMMC Third-Party Assessment Organizations. The process document had also been keenly awaited by many of the more than 200,000 contractors and subcontractors that will have to obtain cybersecurity ratings under CMMC to help them implement their cybersecurity programs.

But the 33-page predecisional draft document, which Cyber AB officials have said is about 80% complete, isn't what many defense contractors hoped it would be. The document is simultaneously overly complicated in some areas while lacking important details on other issues, said Greenberg Traurig LLP shareholder Jeffery Chiow.

"I think it probably leaves people with a couple of reactions. One, this is kind of sloppy, and surprisingly disconnected from the [cybersecurity] tools that have been touted by [the National Institute of Standards and Technology] and DOD," he said. "And two is, oh my God, if it takes this many pages to explain how people are supposed to enter into an agreement with the third-party certification authority, how complex is the evaluation going to be?"

Under CMMC, the DOD will eventually attach minimum cybersecurity ratings to all its contracts, from "foundational" Level 1 for basic compliance requirements, which can be self-assessed, through "expert" Level 3 for the most complex requirements and sophisticated contractors, which will involve an assessment by the government, according to the DOD. C3PAOs are part of the assessment process for contractors at Level 2, the "advanced" level.

The draft version of the plan offers further clarity on issues such as how contractors' use of external cloud providers will be assessed, said Crowell & Moring LLP associate Michael Gruden, a former DOD contracting officer.

"There are a lot more directions that are given and a lot more authority that's going to be given to assessors to review, authenticate and verify how companies are utilizing and adequately meeting the various cloud service standards," he said. "Before, it was a bit more nebulous. It wasn't as clearly defined, as there were more implied requirements, but here there's a lot more specificity."

Other useful details include specifying that contractors can keep the controlled unclassified information that they are supposed to protect in specific "enclaves" within their broader networks, said Holland & Knight LLP partner Eric Crusius.

But "there's still some details to be filled in … perhaps those details are in the dependencies that we don't have our hands on yet," Crusius said, such as appendices referred to in the draft that aren't actually included with the document, or at least the public version of the document, making it hard for contractors to fully determine how they're going to be assessed.

Also, while the draft process helpfully specifies that contractors will be able to get a conditional certification allowing them to use a plan of action and milestones that gives them up to 180 days to address processes that are not yet fully CMMC-compliant, it's not clear whether they will be eligible for DOD contracts with conditional certifications, Crusius said.

"I suspect the answer is yes, because why would they have that program, if not?" he said. "But what happens if a contractor fails to close out those open items? Will they lose their contract? If there's a disagreement on whether or not an item's been closed out, how does that disagreement get adjudicated?"

Given the high potential stakes of losing provisional certification or of failing to get certified at all, such as being cut off from contracts worth millions or even billions of dollars, significant disagreements between contractors and assessors are likely at some point, according to Crusius, but the proposed appeals process for certifications is in an appendix that isn't included in the public draft.

Another issue is that the draft specifies that assessments will involve a contractual arrangement directly between the C3PAO and contractor, with the Cyber AB saying there is "latitude" both in how those agreements are structured and in the specific terms and conditions included.

The related negotiation process could take weeks or even months, pushing out the timeline to complete assessments, especially if C3PAOs are juggling multiple contracts at the same time, according to Hogan Lovells counsel Stacy Hadeka. It could put some contractors, particularly smaller and less sophisticated companies, at a disadvantage in negotiating contractual terms and pricing, according to Hadeka.

"I could see companies that are more sophisticated who engage in these third-party assessments or consultant agreements will be better off in understanding how they'd want to shape those agreements, whereas those companies that haven't really used or leveraged third parties in the past may be at a disadvantage," she said.

For some smaller companies that require Level 2 certification, the cost and complexity of complying with the detailed assessment process may call into question continuing with defense contracting, said Amy Hoang, co-chair of Seyfarth Shaw LLP's government contracts practice group.

And with the draft currently open for comment until Aug. 25, it's also not clear what or how much will be changed, leaving contractors potentially using resources preparing for assessment procedures that

may not be included in a final version at all, according to Hoang.

"It struck me as similar to the evolution of the CMMC framework itself," she said. "Companies started preparing for the CMMC process, which initially required third-party assessments for all certifications, across five maturity levels, only to have CMMC 2.0 revamp that process."

CMMC Version 2.0 is the current, more streamlined version of the program, unveiled in November 2021 in response to hundreds of comments on an initial interim rule. Among other changes, it consolidated five proposed assessment levels into three.

Ultimately, Chiow said, the assessment process should be refined so that it is more of a risk-informed assessment of, as the CMMC name suggests, the maturity of contractors' cyber defense programs and less of a "checklist approach."

Otherwise, one potential consequence of Cyber AB's "missteps" in the draft assessment document is that companies already reluctant or tardy to start to comply with CMMC may use the draft as "an excuse to say that this is not ready for prime time, and you can't force this upon industry," possibly delaying the rollout of the program, according to Chiow.

"That's an unfortunate message to send because there is a real threat — the defense industrial base is under consistent attack by our adversaries, who are accessing defense technologies and other trade secrets and using them against us," said Chiow, a former military officer. "And so we ought to do something that truly does elevate the security posture of the defense industrial base."

Even with the gaps and uncertainties in the draft, and the fact that DOD contracts won't include CMMC requirements for some time yet, it could still be useful for contractors to choose to voluntarily receive assessments from C3PAOs ahead of the process being finalized, several attorneys said.

That could give contractors an opportunity, for example, to see how the assessment process will work, and extra time to address any perceived issues, those attorneys said.

It may also allow contractors to obtain a certification, valid for several years, based on the current version of the National Institute of Standards and Technology's Special Publication 800-171, the cybersecurity standard that underpins much of CMMC, rather than the pending makeover of that NIST document that is expected to add new requirements that may be included in the interim rule implementing CMMC Version 2.0, currently due around May 2023.

In the meantime, contractors will be looking for "real transparency" on CMMC, including potentially additional public listening sessions, similar to when DOD first rolled out the program, and details on issues such as how it plans to help companies that "for a variety of very legitimate reasons aren't able to meet the requirements of the CMMC process but want to continue to work with the government," said Evan Wolff, co-chair of Crowell & Moring's privacy and cybersecurity group.

"There's a lot to do from [both] an industry and a government perspective," he said.

--Editing by Robert Rudinger and Jay Jackson Jr.
