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 Cybersecurity Overhaul Creates New FCA Risk

By **Daniel Wilson**

Law360 (November 5, 2021, 11:03 PM EDT) -- The U.S. Department of Defense's proposed overhaul to its contractor cybersecurity requirements should be simpler to comply with than the previous version, but a purportedly beneficial allowance for self-assessment comes with an increased risk of False Claims Act liability.

Cybersecurity Maturity Model Certification 2.0, introduced Thursday after a monthslong departmental review, is intended to streamline the CMMC program and reduce compliance burdens on defense contractors and subcontractors, the DOD said, including by heavily limiting the previous requirement that all contractors get third-party certification for their cybersecurity programs.

But allowing contractors that don't handle particularly sensitive national security information to self-assess and self-attest their cybersecurity compliance also opens up the potential for FCA lawsuits, as they can no longer in effect "sell their risk" to the outside assessor that signs off on their compliance program, said Holland & Knight LLP partner Eric Crusius.

"That leaves a lot more room for second-guessing down the road, whether it be from whistleblowers or from the government," he said.

While CMMC 2.0 somewhat simplifies a complex certification process, self-assessments also bring subjective interpretation into what often are "deliberately vague standards being applied in a really confusing, complex context," which lack the pass-or-fail clarity of third-party certification, said Crowell & Moring LLP partner Kate Growley, part of the steering committee for the firm's privacy and cybersecurity group.

The risk of potential FCA lawsuits is especially acute after the U.S. Department of Justice launched its high-profile Civil Cyber-Fraud Initiative in October, putting increased emphasis on contractors that "put U.S. information or systems at risk," while also encouraging whistleblowers to come forward with related claims.

The DOJ has put a strong emphasis, for example, on the swift reporting of cybersecurity incidents, and any defense contractors previously reluctant to report incidents under cybersecurity rules will need to rethink their stance, said Rogers Joseph O'Donnell PC's cybersecurity and privacy practice group co-chair Bob Metzger, who co-authored a 2018 MITRE Corp. report that helped underpin the creation of CMMC.

"With this national emphasis on timely reporting and the DOJ's new initiative, there will be many more

reasons for companies to act quickly and promptly in deciding what to report and when, and there's risk … should any company knowingly determine that an event has occurred and decide not to report it," he said.

Although the DOD has suspended its current pilot rollout of CMMC and said CMMC 2.0 won't go into effect until it issues its related rules, typically a nine- to 24-month process, it is unlikely the DOJ will pull back from its focus on cybersecurity issues in the meantime, according to Growley.

"It's still TBD to see how the two will intersect when CMMC 2.0 actually goes into effect, but I think most of the industry expects that this emphasis on cyber-related fraud is not going to be temporary — it will be enduring, and presumably enduring into the timeframe when CMMC 2.0 becomes a real, live requirement," she said.

Another key aspect of the self-assessment process is that related affirmations will need to be made by a senior company official, potentially raising the profile of cybersecurity within contractors and the potential for personal liability for those officials, another area where the DOJ has placed increasing focus under the Biden administration.

Therefore, despite the theoretical cost savings from self-assessment, many contractors that have that option are likely to continue to use an outside cybersecurity expert for regular assessments, helping shore up their good-faith basis for any attestations regarding compliance, Crusius said.

"Because if there is some kind of breach or issue down the road, and they haven't done that, there's going to be a lot of recriminations to try to figure out what exactly the company did and why they felt comfortable making that certification," he said.

Contractors are expected to welcome the elimination of CMMC-unique requirements in version 2.0 of the program, which the DOD said will follow the well-established and widely used standards set out by the National Institute of Standards and Technology's special publications 800-171 and 800-172.

The compression of what had been five levels of increasingly stringent cybersecurity compliance requirements into three — "Foundational" Level 1, "Advanced" Level 2 and "Expert" Level 3 — will also simplify compliance, although it is unclear how the DOD will decide what is a "prioritized" Level 2 acquisition, which will require a third-party assessment, and what is a "nonprioritized" acquisition, allowing for self-assessment.

Also unclear is whether there will be a codified process for when a Level 2 contractor that previously opted for self-assessments decides to pursue a contract opportunity requiring certification from a CMMC Third-Party Assessor Organization, or C3PAO, said Hogan Lovells senior associate Stacy Hadeka.

"Does that mean the company then can just go to the CMMC [Accreditation Body] seeking certification from a C3PAO and they'll be front of line, and there won't be a backlog, and they'll be able to get assessed just by saying that they're interested in the potential opportunity?" she said.

Likely to pique the interest of contractors is the new allowance for awarding a contract even if the contractor doesn't meet all cybersecurity requirements at the time of award as long as they have a plan of action and milestones, or POAM, in place for compliance, as well as the DOD's note that it is "exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC certification in the interim period."

That could mean, for example, a certification a contractor chooses to seek out before the CMMC rule goes into effect is something the DOD recognizes as a "competitive discriminator" in contract solicitations, according to Metzger.

"Personally, I think it's more important to emphasize the incentives to good cyber conduct than it is to threaten the penalties for bad conduct," he said.

Going for voluntary early compliance is especially likely for those that already meet the National Institute of Standards and Technology standards and may not need to do much for CMMC certification, as well as those "hoping to leverage it for marketing purposes," Hadeka said.

"From a business perspective, it makes sense to be able to say that they are CMMC-certified," she said.

Whatever the final version of CMMC 2.0 looks like, it is unlikely to be the last changes the DOD makes, as the implication of rising version numbers is there will be a CMMC 3.0 and beyond, according to Growley. The next version may hew more closely to the more DOD-specific requirements the department had originally intended, she said.

"The DOD often uses the analogy of, 'We're going to do a crawl, walk, run approach,'" she said. "I think DOD in its move to the 2.0 program has acknowledged that industry wasn't ready to run yet. And that suggests that at some point in time, industry will be expected to run."

--Editing by Philip Shea and Michael Watanabe.
