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

Contractors Seek Clarity On DOD Cybersecurity Rule

By **Daniel Wilson**

Law360 (September 29, 2020, 10:28 PM EDT) -- Defense contractors are grappling with a new rule requiring them to implement cybersecurity programs that leaves crucial questions unanswered, including the exact information companies will be required to safeguard and how the new obligations will be worked into contracts.

The interim rule, formally published by the U.S. Department of Defense on Tuesday, explains how contractors will be assessed for compliance with the Cybersecurity Maturity Model Certification framework, the DOD's plan that will eventually attach minimum cybersecurity requirements to all of its contract solicitations.

Improving cybersecurity standards across the DOD's supply chain is intended to help better protect "controlled unclassified information" and other sensitive information from falling into the hands of other countries, amid increasingly numerous and sophisticated cyberattacks, the department said.

But the exact definition of CUI is a key question underpinning the CMMC framework for which the answer remains unclear, one of several key issues that contractors want more clarity on following the release of the interim rule.

What Is CUI?

The protection of CUI forms a core part of CMMC's purpose. Although the DOD first introduced regulations intended to protect that information several years ago, a firm definition of what the department considers CUI remains elusive, with the interim rule providing no new guidance on that issue.

"Bottom line, they still have never defined CUI in a way that's meaningful," Covington & Burling LLP partner Susan Cassidy said. "It's the bedrock of the whole rule. And contractors really want to comply, I believe. They don't want their systems to be hacked. But the definition really should be addressed head on."

Standards for CUI that are currently being provided to contractors range widely. At one extreme, agencies have suggested at times that every piece of data related to a particular program should be

considered CUI, according to Jason Timm, the assistant vice president for national security policy at industry group the Aerospace Industries Association.

At the other end of the spectrum, agencies have suggested at other times that the contractor, as the developer of a system, should be the one to define the relevant CUI that needs to be protected, Timm said. Neither provides a good answer to the question of what CUI actually is, he said.

The lack of clarity on what information the DOD considers important and in need of protection not only affects contractors' approach to how they protect their own information technology systems, but also how they determine what cybersecurity requirements they will need to "flow down" to their subcontractors, as the rule extends down the entire defense supply chain.

How Will CMMC Requirements Be Implemented?

The interim rule also indicates that there isn't going to be any standard template for how CMMC requirements will be included in procurements. Some contracting officers, out of an abundance of caution, could for example err on the side of more stringent cybersecurity requirements than contractors may believe are necessary.

It is also unclear whether meeting the minimum cybersecurity standard for a particular contract will be a strictly pass or fail issue, or whether contracting officers will be able to consider a vendor with a higher CMMC level than the minimum specified as having a competitive advantage.

CMMC certifications run from Level 1, covering basic "cyber hygiene" practices such as regularly changing passwords, through to Level 5, which the DOD has said will involve "proactive" and advanced cybersecurity practices.

Then there are timing-related issues that are still ambiguous, such as whether a prime contractor has to certify that a subcontractor meets a certain CMMC level at the time the prime contract is awarded. Another issue is whether a contractor can apply for an upgraded CMMC level certification in between the typical three-year assessment cycle, if they've upgraded their cybersecurity program in the meantime.

Also, although the interim rule says it will allow contractors to challenge a CMMC assessment if they think the level they were given was incorrect or unfair, that process is not clearly spelled out in the rule.

It is important for the DOD to make the CMMC as clear a model as possible not only for its own sake, but also as a possible example for other federal agencies to follow, as the General Services Administration has already suggested it may do in future. Among other benefits, that would provide contractors that work for multiple agencies a more uniform goal to aim for with their cybersecurity programs, Timm said.

"When one federal agency steps out in front of all the others, and does something that is more detailed than the other federal agencies do, that can cause some ambiguity across an industry member's federal

contracts," he said. "We've asked the DOD what other federal agencies are doing, and if they're not doing something like this, maybe they could start working on bringing the efforts together."

How Much Will Compliance Cost?

Further complicating matters, the DOD may also have underestimated how much it will cost contractors to comply with CMMC, as it has done in the past with other rules related to cybersecurity, McCarter & English LLP government contracts practice co-chair Alex Major said.

"Like with a lot of what we've seen so far ... when it comes to assessing and addressing cybersecurity, the expectations in terms of costs by the government don't necessarily meet the demands facing contractors," he said. "It is unfortunately a very expensive endeavor … a necessary endeavor, but that also is one of the reasons that it is so expensive."

The cost estimates in the rule work off an assumption that contractors will be assessed every three years, averaging out costs to about $1,000 per year to meet Level 1, ramping up to about $480,000 per year for Level 5.

But that doesn't take into account the potential for more rapid reassessments, for example where a contractor's system or the data it holds is so sensitive that the DOD may require them to recertify more frequently or when they make a change to the underlying system, Stinson LLP partner Susan Warshaw Ebner said.

It also may not fully take into account the costs of upgrades a contractor needs to stay at a given CMMC level. Cybersecurity threats continue to evolve and what is considered to meet a particular level now may not meet that level in three years as the DOD updates the underlying CMMC framework, Ebner noted.

And the rule suggests that small businesses typically have smaller networks that are less costly to protect, but that doesn't take into account that some small businesses may have particularly secure or important data that requires one of the higher levels of CMMC certification.

The estimated cost assessment is also limited to CMMC-specific costs, excluding the costs of complying with the National Institute of Standards and Technology's Special Publication 800-171, which underpins the DOD's existing, more narrow rule for protecting CUI and also forms the basis for four of the five CMMC certification levels.

While the DOD presumably expects that contractors will have met the existing standard, some contractors are currently deemed compliant only because they have a plan in place to hit the target at some point in future, which won't count under CMMC, according to Ebner.

"They don't account for any of the costs of that, which I think are going to be significant still to have contractors get up to speed," she said.

Next Steps

The interim rule goes into effect in 60 days, with comments on the rule open during that period and a final rule to follow further down the track. CMMC, however, won't apply to all DOD contracts until October 2025, which gives contractors some breathing room.

In the meantime, the office of the undersecretary of defense for acquisition and sustainment will decide which procurements will have CMMC requirements attached, essentially a pilot program that can be ramped up over time as more contractors are assessed and given CMMC certifications.

"Presumably, you think they'd do a mix [of different types of contracts] so they can work out any kinks in the system," Cassidy said. "I think that is a good thing, because if you left it to the [DOD] departments, you would run into the risk that there would be too many, too quick."

--Editing by Emily Kokoll and Aaron Pelc.