Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How A Cybersecurity Proposal Could Expand FCA Liabilities

By **Daniel Wilson**

Law360 (October 4, 2023, 9:02 PM EDT) -- Newly proposed cybersecurity regulations imposing new reporting and compliance requirements may expand the ways in which federal contractors, including companies that aren't currently subject to such requirements, could face liabilities under the False Claims Act, experts say.

The Federal Acquisition Regulatory Council on Tuesday published a pair of proposed rules ramping up cybersecurity requirements for contractors: one standardizing contractual cybersecurity requirements across the government for "unclassified federal information systems," and the other requiring contractors to share information on cybersecurity threats and report cybersecurity incidents to the government.

The proposals are broad, applying to the majority of federal contracts and to companies otherwise exempt from many contracting rules, and come with strict requirements and timelines that open up potential vectors for FCA liability for unwary contractors, explained Hogan Lovells counsel Stacy Hadeka.

"Both of the proposed rules underscore, and actually explicitly state in the rules, that the cybersecurity requirements and incident reporting requirements are material to eligibility and payment under government contracts," she said. "So both the rules ... are trying to get that hook in there for False Claims Act implications."

While many contractors are already subject to cybersecurity requirements, particularly those who work with the U.S. Department of Defense, the new rules will sweep in many more, such as sellers of commercial off-the-shelf or low-value items, according to Crowell & Moring LLP counsel Michael Gruden.

"I think there's definitely going to be a significant impact," he said. "I think many companies that thought that they were not required to monitor [cybersecurity issues] closely ... are now being brought into the fold of cyber compliance incident reporting."

Among the regulatory clauses that could affect contractors is a requirement to report all cybersecurity incidents within eight hours of discovering them, much shorter than the DOD's 72-hour deadline. That proposed deadline will likely be practically impossible to meet for contractors who don't have related processes in place already ahead of an incident, said Jeffrey Chiow, co-chair of the government contracts practice at Greenberg Traurig LLP.

"As I read it, in order to be able to meet that eight-hour incident reporting rule, [the FAR Council expects] that you're going to have, essentially, either signed up for an automated information-sharing capability

through [the Cybersecurity and Infrastructure Security Agency], or that you will have entered into an automated information-sharing program that accomplishes the same objective," he said.

There is also a proposed annual certification requirement in which contractors must effectively state that they have complied with their cybersecurity reporting obligations. That could be a "very powerful tool for the government," particularly in light of the U.S. Department of Justice's ongoing Civil Cyber-Fraud Initiative, under which it has placed more focus on bringing cybersecurity-related FCA cases, Chiow said.

"If they discover a couple of years down the road that you had an incident [and] you didn't report it; you didn't do the things they expected you to do — you've got a certification that said you did," he said. "That's an express certification, and that really simplifies the prosecutor's task."

And alongside potential liability under the FCA, contractors could also be on the hook under a "pretty expansive" indemnification requirement included in the proposed rule standardizing cybersecurity requirements, Hadeka noted, adding that the rule states that contractors must indemnify the government for any liability stemming from "introduction of certain information or matter into government data or ... unauthorized disclosure of certain information or material."

"It puts a lot of the onus on contractors, and ... really stresses the importance of compliance programs, having [related] policies [and] ensuring personnel are trained properly," she said.

There are also a number of unclear, confusing and even potentially unlawful issues across the two proposed rules that could cause concerns for contractors, experts say.

For example, website references included in the rules seem to run afoul of requirements that materials incorporated into rulemaking by reference must refer to a specific edition of a publication, said Wiley Rein LLP partner Gary Ward.

"Here, the government has included the URL for current publications, with the idea that the content of those references will change over time and immediately become binding as they evolve," he said. "I've seen that referred to as 'dynamic incorporation,' and courts have found it unlawful in other contexts."

Another murky issue is how to address disparities between the FAR Council's incident reporting requirements and the DOD's existing reporting requirements, which could require a "sophistication and nimbleness in navigating IT forensics and legal analysis" for contractors subject to both sets of rules, according to Gruden.

"I don't think it will be a simple 'pull the lever and issue a hybrid incident report'; it's going to take a lot more careful analysis before determining which notifications need to be issued to the government based upon the actual incident that occurred," he said.

Also currently unclear but crucial to how the pending rules will be implemented is exactly what counts as an "information and communications technology" system. The proposed cybersecurity incident reporting requirements will apply to all contractors who use or provide such systems under their contract, a group the FAR Council said it anticipates will include 75% of all federal contractors.

"We're going to need such clear language there," Chiow said. "Because in the absence of clarity, you have to, I think, assume that if I take any federal government contract of any value, no matter what I'm doing — [say] I'm delivering pencils [and] I use an ordering and online ordering system for delivery — I bought

some serious obligations. It's got to be real clear if there's any way to avoid having these rules apply to you."

But a positive move for contractors, which stands in contrast to many other significant recent federal contracting policies, is that the rules were issued as proposals and not as interim rules, according to Ward. That will at least give contractors an opportunity to weigh in on aspects of the rules that they find ambiguous or concerning without being subject to those requirements in the meantime, he explained.

"That was not a given," Ward said. "From watching this [space] over the last decade, we've seen the government implement a lot of significant policies through interim rules that become effective immediately in their original form — interim rules really have started to become the norm rather than the exception. With the cybersecurity rules, we're finally starting to see the FAR Council embrace the process that is more common in other regulated environments."

The FAR Council has also asked for feedback on specific issues in the rules, such as a requirement that contractors give the FBI and CISA access to their information systems, which Ward said he hoped was "a sign they are really interested in considering that input and getting the contractors' perspective."

The rules will be open for public comment for 60 days.

--Editing by Alanna Weissman and Emily Kokoll.
