Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

DOD's Cybersecurity Rule May Help Fend Off FCA Claims

By **Madeline Lyskawa**

Law360 (September 9, 2025, 11:18 PM EDT) -- The U.S. Department of Defense's requirement for certain contractors to have a third-party assessor review their cybersecurity compliance, implemented in a final rule Tuesday, could help contractors protect themselves from False Claims Act enforcement.

The Pentagon laid out its three-year implementation plan in a final rule to phase in requirements in the Cybersecurity Maturity Model Certification program, which went into effect in December and attaches one of three levels of cybersecurity requirements to nearly all defense contracts and contract solicitations.

Most contractors subject to CMMC Level 2 are required to have their cybersecurity compliance verified by outside assessors known as CMMC Third-Party Assessor Organizations. The DOD estimated that approximately 118,289 entities will need to secure this third-party certification by the end of the three-year implementation period.

While this requirement could prove to be burdensome for small and midsize contractors who handle controlled unclassified information, Jacob Harrison, a government contracts associate with Crowell & Moring LLP, told Law360 that the program's third-party validation requirement could also help contractors lessen their risk of facing an FCA case from the U.S. Department of Justice.

The DOJ has made an increasingly concerted effort to use the FCA to combat cybersecurity weaknesses among defense contractors, reaching an $8.4 million settlement in May with Nightwing Group, Nightwing Intelligence Solutions, RTX and Raytheon to resolve claims that the companies falsely certified their cybersecurity compliance between 2015 and 2021, while performing on 29 defense contracts.

The DOJ struck another $4.6 million settlement with defense contractor MORSECORP Inc. in March to resolve an FCA suit claiming the company submitted invoices to the DOD despite knowing its third-party email system was not compliant with federal cybersecurity standards.

In these types of cases brought by the DOJ, Harrison said the agency often argues that defense contractors either ignored or overlooked cybersecurity deficiencies when assessing their own compliance. But as more and more contractors become subject to CMMC and have their cybersecurity compliance verified by a third-party assessor, Harrison said they can credibly say they had an expert come and assess their compliance.

"I think the key there, though, that DOJ will be focused on, is that companies need to be forthcoming

with their assessors," Harrison said.

Eric S. Crusius, a government contracts partner at Hunton Andrews Kurth LLP, came to a similar conclusion, saying while getting a third-party assessment doesn't eliminate the risk of FCA enforcement, it can certainly help to lower that risk substantially.

"If a company is accurate in the scope of their system, and they get that system assessed by an authorized third party, and that assessment is successful, it's very difficult for the government to argue that the company did something wrong that would warrant a False Claims Act action, unless there was some kind of obfuscation by the company in the assessment process or in defining the scope of the assessment," Crusius said.

CMMC also provides contractors with the full suite of cybersecurity requirements that DOD is expecting them to meet when handling controlled unclassified information, which they can become intimately familiar with to ensure compliance and protect themselves against FCA enforcement, Michael G. Gruden, a government contracts and privacy and cybersecurity partner with Crowell & Moring LLP, said.

"Does that fully mitigate [risk]? No, but I think that the positive is that there's full clarity now and there's sort of less of a guessing game," Gruden said.

But while third-party assessors can help with ensuring compliance, Ryan Burnette, a special counsel with Covington & Burling focused on government contracts and technology, said companies also need to make sure that they don't run afoul of their compliance certification by making changes to their systems after having a third-party assessment.

"Companies really have to focus closely on these requirements and not only make sure that they're implementing them as the rule goes into effect, but also maintaining implementation of these requirements going forward as they do business with DOD," Burnette said.

Moreover, Stacy Hadeka, a government contracts partner with Hogan Lovells, said the same third-party validation requirement can also make it more difficult for small businesses to participate in government procurements.

"It comes down to the ability to have documentation that you're complying with these requirements, the ability to pay extra money, possibly, to ensure that you have a FedRAMP Moderate cloud solution that you're leveraging, if that's what you use for storing or transmitting any [controlled unclassified information], and it can be a big investment," Hadeka said.

As a result, some companies may choose not to become CMMC certified and move onto other avenues of opportunity, Hadeka said.

--Additional reporting by MJ Koo and Parker Quinlan. Editing by Jay Jackson Jr. and Emily Kokoll.
