INSIDE CYBERSECURITY

DAILY NEWS

Defense Dept. to require new cybersecurity certification from contractors

June 03, 2019 | **Justin Doubleday**

The Pentagon will unveil a new cybersecurity certification for its contractors this year, as Department of Defense officials concede the current rules governing how companies should secure sensitive information are not working.

The new standard is called the "Cybersecurity Maturity Model Certification," or CMMC, according to Katie Arrington, special assistant for cybersecurity in the office of the under secretary of defense for acquisition and sustainment.

"Every single business doing any kind of business with the Department of Defense will need to get certified and get a third-party audit that they have basic cyber hygiene," Arrington said during a May 23 cybersecurity conference hosted by the Georgetown University Law Center in Washington.

In developing the certification, DOD has looked at how the United Kingdom and Australia approach the issue, Arrington added.

The United Kingdom requires government contractors handling sensitive information to get a "Cyber Essentials Certification," while Australia employs an "Essential Eight" mitigation strategy for organizations to prevent cybersecurity incidents.

DOD is moving to the new CMMC model due to continued cybersecurity deficiencies in the defense industrial base, according to Arrington.

"I think one of the bigger problems we have is cyber hygiene, and we think that we're doing it, but we're still getting phished, we're still vulnerable to ransomware," she said. "We need to evolve. Our adversaries are doing that."

The CMMC is intended to serve as the enforcement mechanism lacking in the current Defense Federal Acquisition Regulation Supplement. The DFARS rule says contractors handling sensitive, unclassified information should protect it in accordance with the 110 security controls laid out by the National Institute for Standards and Technology special publication 800-171.

But the rule only requires contractors to self-attest to their compliance by documenting a current "system security plan," as well as a "plan of action and milestones" for satisfying any unimplemented NIST controls. A recent report found many defense contractors are struggling to implement most of the controls.

The DFARS rule flows down from prime contractors to all subcontractors handling covered defense information. But Arrington said DOD has found the largest defense companies -- the "big six" defense contractors, which often act as the prime contractors on major acquisition programs -- haven't been enforcing the rules down their supply chain.

"We audited some of the big six," Arrington said. "We were finding that they weren't really flowing down the requirement, and the self-attestation is not working. "If it was, our adversaries wouldn't be flying a particular plane around that looks really like an F-35," she added.

DOD officials have for the last several months discussed "scoring" contractors against new cybersecurity standards, and Pentagon acquisition chief Ellen Lord said she aims to begin auditing contractor cybersecurity next year.

Lord's office is leading the development of more stringent contracting language to hold companies "accountable" for their cybersecurity, and Arrington confirmed the CMMC is at the center of the development.

"Once you're certified and audited, if there is an [exfiltration] that has happened and you have followed process, absolutely we understand that," Arrington said. "But if you have been negligent, we as taxpayers are all paying that bill."

The idea of using third-party audits to certify contractors is a "sea change" compared to the current rule's reliance on self-certification, according to Evan Wolff, a partner in law firm Crowell & Moring's Washington office and co-chair of the firm's Privacy & Cybersecurity Group.

"I think some companies will find it welcome," Wolff said. "Some companies will find it disheartening. I think many companies will say that this is inconsistent with the regulatory authority, that it doesn't match how the rule is written."

While the current rule offers flexibility in how companies implement the NIST standards, it also comes with the uncertainty in how different DOD organizations will interpret and measure a contractor's adherence to the security controls, according to Kate Growley, counsel in Crowell & Moring's Washington office.

"One of the benefits that some people have been talking about with this third-party certification is the certainty that it brings to the process," she said.

But in order to implement the new requirements, DOD will likely need to at least revise the DFARS rule, according to Growley.

The Pentagon did not respond to questions about the CMMC and how it plans to implement the new certification.

It's also not yet clear to what extent the NIST controls will be featured in the CMMC. Lord has previously said DOD's new cybersecurity standards will draw on the "NIST framework."

But John Luddy, vice president for national security policy at the Aerospace Industries Association, said the CMMC is also based on a new standard for cybersecurity released by AIA in December. Luddy has been among industry representatives meeting with DOD officials on the issue of contractor cybersecurity over the past several months.

The AIA standard, called the "National Aerospace Standard 9933: Critical Security Controls for Effective Capability in Cyber Defense," takes "Critical Security Controls" and categorizes them into five capability levels. Capability Level 3 is considered the "minimum performance level" for defense contractors, while Category Levels 4 and 5 consist of "higher-level objectives," according to AIA's website.

"Instead of the [NIST] 801-171 checklist, DOD has taken our approach of a more dynamic model that does adapt to different kinds of threats," Luddy said.

DOD is due to complete a draft version of the CMMC sometime in June, according to Luddy.

Beyond what's in the certification, the success of the new initiative will hang on the Pentagon's implementation of the CMMC and third-party auditing measures across its vast industrial base, according to Robert Metzger, head of the DC office for law firm Rogers Joseph and O'Donnell.

"The mechanism of getting the CMMC accomplished for the entirety of the defense industrial base at all levels of the supply chain? That's the crucial question," Metzger said. "Even if the idea is elegant, it must be accompanied by a workable and scalable implementation method, or else it will prove a great concept with little less than desired practical benefit."

DOD could begin piloting the use of the CMMC and third-party auditors this year, he suggested, by using other transaction agreements to test out different methods of certification. He said the Pentagon could also direct the military services to select different programs and contracts to serve as pathfinders for the new certification requirements.

"We need to try a number of things concurrently on a determined schedule, with a plan to assess the results hopefully within this calendar year," Metzger said. "So by the end of the year or early next year, we have an informed basis to choose the methods that will be scaled out and expected of more companies."

But requiring companies to be certified before they compete for defense contracts -- what officials call a "go or no-go" regime -- will likely result in some smaller subcontractors being deemed ineligible, according to Growley.

"A lot of primes and higher-tier subs who rely on several, smaller subcontractors to provide those products or services might find themselves in a position where a good chunk of their supply chain is a no-go," she said.

But even if that's the initial effect of the new CMMC, other companies should fill in the gaps.

"I think the short-term reaction will probably be some shrinking of the pie, and then also probably some increased expenses associated with that," Growley continued. "But as the market has done in several other instances, there will probably be an adjustment period after that."

With cybersecurity threats to the defense industrial base only growing, Luddy said "it almost doesn't matter" whether some companies are temporarily or permanently forced out of defense contracting due to strict cyber audits.

"It's hard for me to sit here and argue that because this is going to be tough on industry and might in fact drive some people out of the business, that we shouldn't do it," Luddy said. "I think we're going to have the resources across the industry to keep companies in the business if they want to be OK. The talent is there, the tools are there, the will is there. We'll be able to get the key people engaged if they want to stay engaged. None of this is impossibly hard to do." – *Justin Doubleday (**jdoubleday@iwpnews.com**)*

10015

RELATED NEWS

- **Kaspersky researcher: DHS move on products was reasonable, but congressional ban on services was self-defeating**
- **Huawei cites U.S. cybersecurity policy in challenging constitutionality of ban**
- **CISA chief Krebs says supply-chain security will come to dominate cyber agency's agenda**
- **Krebs says NRMC risk review will be narrowed to respond to Trump supply-chain order**
- **Report: DOD contractors continue to struggle with cybersecurity requirements**