DOD Cybersecurity Maturity Model Certification Offers Alternative to Compliance Checklists

Public and private-sector efforts now have a tiered approach to cybersecurity controls.

James Mersol

Wed, 04/01/2020 - 14:55

Photo Credit: Matejmo/iStock

As part of its effort to increase supply chain security across the board, the Defense Department has developed the Cybersecurity Maturity Model Certification (CMMC) to certify vendors' cybersecurity controls in the unclassified space. CMMC is designed to ensure that every vendor in the defense industrial base is taking steps to secure its systems and controlled unclassified information (CUI). Rather than focus on meeting a certain number of standards or achieving a level of compliance, the CMMC focuses on implementing a range of controls and cyber hygiene practices, which will be evaluated by third-party assessors and scored based upon levels of maturity.

The current guidelines underscore that the framework is part of an effort to reduce the estimated $600 billion loss to the U.S. economy due to IP theft, economic espionage and other forms of malicious cyber activity. While the defense industrial base is not the sole target, cybercrime and other malicious activity represents not only an economic threat, but also a threat to national security.

The CMMC is not meant to be a new checklist, explained Katie Arrington, chief information security officer for the Defense Department's Assistant Secretary for Acquisition, but a metric for DOD to evaluate vendors' cybersecurity programs across five levels of maturity.

Level 1 consists of "basic, low- or no-cost" measures that every company should be able to perform.

"If you're listening to this webcast, you should be doing these things," Arrington said on a webinar April 1.

Vendors must achieve at least level-three certification to do business with the DOD. It is a major leap from level one, requiring that vendors implement incident reporting mechanisms, encrypt all CUI on mobile devices and 111 other measures. These measures are essential for “good cyber hygiene,” but may be difficult for a small business to implement, Arrington explained. CMMC level two was designed as an intermediate step for those businesses, requiring only 55 of the 113 measures between levels one and three, including implementing “the principle of least privilege” and monitoring remote access on company systems. Even if levels one and two are not enough to access DOD CUI, they are important for businesses to chart their progress on the path to a level-three certification, rather than receiving a notification that they do not yet meet the level-three standard.

Arrington emphasized that the CMMC is still under development and that to date, no vendor has a CMMC certification nor is an accredited auditor. She also dispelled the myth that any vendor is “NIST certified.” While the CMMC is based upon the existing National Institute for Standards and Technology (NIST) Special Publication 800-171, NIST does not offer certifications.

Once the CMMC framework is implemented, vendors in the defense industrial base will have the opportunity to have their entire enterprise network certified at one of the five levels or focus on certification for one segment if that is more practical for their business, CMMC 1.0 states.

Arrington said she does not expect the COVID-19 pandemic to slow down CMMC development, underscoring that cybersecurity concerns have not gone away, nor will they. For now, DOD is making sure to avoid organizational conflicts of interest (OCI) in how it designs its program. Contractors who assist in designing the specific metrics for CMMC will not be awarded the contract to audit DOD vendors, she said, nor will auditors audit themselves once the framework is in place.

Following CMMC implementation, the pace of acquisition may slow in the short term, but ensuring every business in the defense industrial base is properly certified is essential for long-term security and efficiency.

“We are not going to move to a contract award until everyone who submits a contract bid has an opportunity to get certified,” Arrington said.

View printer friendly version

Defense Department
acquisition
Federal Cybersecurity
Standard