CMMC Accreditation Launch Moving Forward Despite Pandemic, Arrington Says

Though some regulatory procedures have been impacted, accreditation board is already working with industry.

James Mersol
Thu, 05/14/2020 - 15:35

Under Secretary of Defense for Acquisition and Sustainment Ellen M. Lord, Kevin Faheny and Katie Arrington speak at a press briefing at the Pentagon in January. Photo Credit: Defense Department/DVIDS
Spurred on by several national-level reports on cyber readiness and what must be done to improve cybersecurity both in government agencies and for vendors, especially in the defense industrial base, the Defense Department is moving forward with the Cybersecurity Maturity Model Certification. The CMMC is an ambitious program that will allow vendors to gain insight on where their cybersecurity practices are rather than simply passing or failing a compliance review.

“This didn’t come out of the blue,” said DOD Office of Acquisition CISO Katie Arrington.

Rather, both the Cybersecurity Solarium Commission’s March report, as well as reports from the MITRE Corporation and the U.S. Navy informed CMMC’s requirements and the way the DOD is going about establishing training and education. CMMC is also a result of over two years of legislative efforts that have emphasized defense acquisition security.

Although COVID-19 has created some obstacles for implementing CMMC, most facets of the program, including establishing the accreditation body that will be responsible for assessing vendors’ security, are moving forward with little difficulty. Developing those requirements is a critical part of the program, given that they will affect cybersecurity and national security for years to come.

“The premise of all of this is that we’re doing a DFARS [Defense Federal Acquisition Regulation Supplement] rule change,” Arrington said.

Under the original plans for CMMC rollout, public hearings regarding the DFARS change would have occurred in early May. The technologies and procedures for those hearings are not currently in place; nevertheless, Arrington emphasized that this hurdle has not affected her office’s work on training and accreditation. The next step, she said, is working with industry to understand where vendors of all sizes are in their cybersecurity programs and ensuring they know how to proceed.

“I don’t believe for a second that where we are in cybersecurity is out of intent,” Arrington said, underscoring that there are known flaws in mission-critical systems in the DOD — including in weapons systems — and fixing those is of the utmost priority. Arrington expects that the current pandemic is only heightening the importance of improvement.
“World War II changed the way we build things,” Arrington underscored. “9/11 changed the way we moved. COVID has changed the way we interact with one another ... cyber has allowed us to [flourish] in the past seven or eight weeks.”

“We embody the rallying cry of: ‘We must make this happen,’” agreed Ty Schieber, board chairman of the CMMC Accreditation Body. “We’re not letting COVID get in the way of our aggressive schedules.”

Most recently, the board identified the CMMC “ecosystem,” to better understand what the accreditation body and auditors should look like and how they will carry out their assessments. Schieber said the board has not yet made a determination on how to carry out training and education online during the pandemic, but as a professor at the University of Virginia, he hopes to offer his insights for making that determination.

Arrington stressed that one of CMMC’s goals is to “change the culture for small business,” recognizing that small businesses are often more nimble and innovative in the defense industrial base than large ones, but can also struggle with knowing how to establish robust cybersecurity programs that meet DOD standards.

All defense industrial base vendors will receive a CMMC grade level between 1 and 5; while DOD RFPs will require a minimum of a level 3 certification, levels 1 and 2 give those small businesses both a clear understanding of where they are in their progress and what steps they need to take to attain the next level.

“We’re trying to reduce costs, not build them,” Arrington said. “We’re trying to reduce bureaucracy and speed up processes.”

Last week, Arrington announced that DOD is working with GSA to ensure there is reciprocity between CMMC and Federal Risk and Authorization Management Program (FedRAMP) certifications. Her office is also establishing a public website to support cybersecurity for small businesses and working with DOD Professional Technical Assistance Centers (PTACs) to help small businesses prepare for audits.

Arrington said that both Undersecretary of Defense for Acquisition and Sustainment Ellen Lord and Defense Secretary Mark Esper have said that it is essential to “make this affordable and easy for small business, because we cannot afford to lose them.”
These comments come amid other updates for the CMMC process. The deadline for mandatory CMMC compliance has been shifted back, with the first RFPs featuring CMMC requirements arriving in November.

“We need to make sure companies have all the resources possible,” Arrington said, “because [the companies] are our national defense.”