DOD Ready to Begin CMMC Accreditations

Defense acquisition's top official brief next plans of certifying contractors according to new cybersecurity standards.

Melissa Harris
Thu, 10/29/2020 - 12:09

The Defense Department will begin rolling out its Cybersecurity Maturity Model Certification (CMMC) framework for all military contractors to undergo assessments starting Dec. 1, DOD Chief Information Security Officer for Acquisition and Sustainment Katie Arrington confirmed.
Arrington expanded on the announcement during C4ISRNET CyberCon Wednesday by sharing that the department is finalizing the CMMC Accreditation Body (CMMC AB) statement of work, which will establish a third-party assessment organization to review CMMC cybersecurity compliance in new military contracts starting in December.

“As of Dec. 1, cybersecurity is in all acquisitions,” Arrington said. “Contracts prior to award need to register their self assessment via [Supplier Performance Risk System] platform, and as we move forward with the CMMC we actually had a meeting today to get ready to release the pilot programs. Each of the services and co-comms and, I want to say, two support agencies, are getting ready to release the pilots and where they’ll be.”

DOD established a memorandum of understanding in March to eventually form the CMMC AB, an organization that would establish a standard for CMMC that would guide its certification of organizations seeking to conduct business with the military based on the new tiered cybersecurity controls that the model is establishing.

Over recent months, the CMMC AB has been training auditors through “pathfinders,” Arrington said, where those individuals underwent provisional training and mock cybersecurity audits using the CMMC guidance.

“This week will be the end of the third tranche of provisional assessors through the accreditation body’s training and assessment period, and as soon as the rule goes into effect on Dec. 1, we can get them from provision to actual, real certification,” Arrington added.

Arrington and her team decided, after receiving feedback from others across DOD as well as academia and industry, to establish three International Organization for Standardization (ISO) certifications in the CMMC AB statement of work. Three of them need to be within two years, which is the standard onboarding process to ensure continuity and meet ethics requirements, she added.

CMMC has five levels of cybersecurity requirements, and each contract will require a certain level that contractors need to meet, where Level 1 corresponds to basic safeguarding requirements established by the Federal Acquisition Regulation, and Level 5 sets the most robust cybersecurity requirements for contractors and suppliers.