wiley

NEWSLETTER

Do Changes Lie Ahead for CMMC Program?

July 2021

A recent hearing before the Senate Armed Services Committee's Subcommittee on Cybersecurity portrayed an uncertain future for the U.S. Department of Defense's (DOD's) Cybersecurity Maturity Model Certification (CMMC) program, including likely changes and delays in final agency action. Coupled with the Biden Administration's recent Executive Order on cybersecurity, it injects new uncertainties for government contractors seeking to comply with the CMMC regime that will eventually emerge, particularly small businesses.

The May 18, 2021 hearing included testimony from Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy, who assumed responsibility for CMMC in February. Salazar's written testimony highlighted three key objectives of the CMMC program, including (i) incorporating a unified set of cybersecurity requirements into acquisition processes and contracting language; (ii) providing the DOD assurance, via external assessment, that all contractors and subcontractors participating in a given award meet mandatory cybersecurity requirements; and (iii) developing supporting resources, information, and training to help contractors improve cyber readiness and comply with the DOD's requirements. Salazar focused frequently on the need for CMMC implementation throughout the supply chain, where Tier-3 and Tier-4 suppliers comprise nearly 75% of the defense industrial base and nearly all are small businesses.

Salazar noted that DOD received more than 850 comments in response to the Defense Federal Acquisition Regulation Supplement (DFARS) interim rule that established CMMC, and estimated that it would take DOD roughly a year to adjudicate those comments and proceed with a final rule. In charting a path forward, he highlighted DOD's focus on three policy considerations:

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Kyle M. Gutierrez
Associate
202.719.3453
kgutierrez@wiley.law

Practice Areas

Cybersecurity

Government Contracts

Managing costs of cybersecurity for small businesses: Salazar stated that small businesses "have told us loud and clear" that they are under financial duress from COVID-19 and industry consolidation, and face "resiliency issues." Salazar pledged that DOD's approach "must balance the need for accountability with a recognition of the challenges facing small businesses." The DFARS interim rule on CMMC does not include any carve-out or exception for small businesses, and it is unclear whether Salazar's testimony is a preview of more flexibility that DOD intends to build into the CMMC regime for small businesses, or more resources that DOD intends to provide to small businesses to share the cost of compliance and assessments. During the hearing, Subcommittee Chairman Senator Joe Manchin (D-WV) echoed the concern that the current iteration of CMMC does not do enough to assist small businesses, either to meet their certification requirements or to prioritize personnel or investments.

Clarifying cybersecurity regulatory, policy, and contracting requirements: Salazar expressed need to "de-conflict and streamline multiple cybersecurity requirements to prevent duplicative assessments." Specifically, he stated this would include providing clearer guidance on how the CMMC and National Institute of Standards and Technology's (NIST's) SP 800-171 DOD Assessment Methodology align with one another for safeguarding controlled unclassified information, and on how those requirements extend to contractors that use cloud-based services. Both of these focus areas will become even more important as the government rolls out new rulemaking in coming months to implement the cybersecurity Executive Order, which calls for new government-wide standards for cloud security, as well as government-wide cybersecurity standards for government contractors. Both pose the risk of increasing redundancies and/or conflicts with DOD's current CMMC and NIST SP 800-171 requirements.

Reinforcing trust and confidence in the maturing assessment ecosystem: Finally, Salazar emphasized that the success of CMMC implementation depends on DOD ensuring that it can "operationalize" with qualified third-party assessors. Because the independent third-party assessor organizations will be the backbone of CMMC certification, DOD needs to confirm it has "sufficient numbers of assessors to deliver independent, rigorous and timely assessments" to support acquisition needs, and that they have "clearly defined roles and responsibilities" with "standards of conduct and audit mechanisms governing relationships with private sector entities within the external assessment system." The latter concern seems to respond to perceptions that have dogged CMMC that the third-party accreditation process could morph into a pay-to-play program. At present, the CMMC Accreditation Body tasked with implementing CMMC has not commenced formal training for any CMMC "Certified Assessors," announcing recently that it hopes to commence the training and certification program beginning "mid-to-late summer 2021." (To date, "Provisional Assessors" are operating under a pilot program.)

This testimony, highlighting potential further delays and changes to any final implementation of CMMC, comes against the backdrop of an ongoing independent review of the program initiated by DOD in March. There is speculation that DOD's internal review—coupled with the momentum of the cybersecurity Executive Order and industry pushback to the independent third-party assessment concept and implementation—could result in substantial changes to the path forward for CMMC. Senator Manchin seemed to signal as much during the hearing.

CMMC's future could also be impacted by a recent report that DOD's head of the CMMC program was placed on leave on May 11, and had her security clearance suspended, amidst government concerns regarding "reported unauthorized disclosure of classified information."

Ultimately, these latest CMMC developments sow doubt about whether the current CMMC framework is aspirational and can be adequately "operationalized." Despite DOD's aggressive timelines when the program was first announced two years ago, few of those milestones have been timely achieved. DOD has been slow to build and deploy the training and guidelines for the third-party assessors, which has prevented DOD from elevating the program much beyond its initial pilot endeavors. We flagged those delays over a year ago, and little progress appears to have been made in the interim. So, while we encourage contractors to continue monitoring any developing CMMC requirements and policies, be prepared for further delays and potential changes, which may be significant.