Government Contracts

Cybersecurity as Acquisition Differentiator: New CMMC and Cybersecurity Interim Rule

By: David B. Robbins, Cynthia J. Robertson, and David Bitkower

Department of Defense representatives have signaled for months that the Department would begin to use cybersecurity as an acquisition differentiator, and a new interim rule brings the DoD one step closer to that goal. This interim rule requires cybersecurity assessment scores (whether Basic Level self-assessments or Medium/High Level government assessments) to be published in the Supplier Performance Risk System. DoD acquisition professionals will have access to the SPRS system, will be able to review assessment scores, and will "verify that an offeror has a current (i.e., not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award." In short, DoD has announced that cybersecurity will be scored and will become a differentiator in future acquisitions.

Additionally, the interim rule further fleshes out the Cybersecurity Maturity Model Certification (CMMC) framework to add a "comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level." While employing slightly different language, this fleshed out model will look familiar to those who were already measuring their cybersecurity maturity against the AICPA/CICA privacy maturity model. CMMC scoring is available for contractors' entire enterprise network or specific portions of networks, and will further enable the DoD to assess cybersecurity as an acquisition differentiator. Levels will be assessed by independent third party assessment organizations. Emphasizing the effort required, CMMC Level 1 consists of the 15 basic safeguarding requirements from FAR 52.204-21 (Basic Safeguarding) and Level 5 consists of all 110 security requirements from NIST SP 800-171, 61 additional CMMC practices, and 5 additional CMMC processes.

The CMMC process will be rolled out in phases, with full implementation no earlier than October 1, 2025, when the appropriate CMMC rating required to be eligible for contract award. The phase-in period offers contractors a period of time to make necessary investments and complete their implementation of DoD's cybersecurity requirements, or risk ineligibility for future contract awards.

Jenner & Block lawyers stand ready to assist contractors in understanding and complying with these emerging requirements.

Contact Us

David B. Robbins
drobbins@jenner.com | Download V-Card

Cynthia J. Robertson

crobertson@jenner.com | Download V-Card

David Bitkower

dbitkower@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

Marc A. Van Allen

Co-chair

mvanallen@jenner.com

Download V-Card

David B. Robbins

Co-chair

drobbins@jenner.com

Download V-Card

D. Joe Smith

Co-chair

jsmith@jenner.com

Download V-Card