Crowell

Client Alert

CMMC 2.0 Scoping Guidance Limits the Scope of Cybersecurity Assessments

December 23, 2021

The Department of Defense (DoD) recently released the initial guidance documents for Version 2.0 of its Cybersecurity Maturity Model Certification (CMMC) program, including its much-anticipated Scoping Guidance. While the guidance documents generally adhere to the current requirements for the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), the Scoping Guidance includes notable developments. Chief among them is the introduction of two asset categories — "Specialized Assets" and "Contractor Risk Managed Assets" — that could potentially limit the scope of a contractor's CMMC assessment, as well as the number and types of assets to be assessed against the applicable CMMC practices.

- Specialized Assets include government property; internet of things (IoT) and industrial internet of things (IIoT) devices; operational technology; systems configured based entirely on government requirements and used to support a contract; and test equipment.
- Contractor Risk Managed Assets include computing resources that are capable of handling CUI but are prevented from doing so by the contractor's security policies, procedures, and practices.

Contractors expecting to be subject to CMMC should carefully review the Scoping Guidance, as well as the other guidance documents, to determine whether and how they may wish to limit the scope of CMMC's applicability.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1.202.624.2596
Email: mlerner@crowell.com

Michael G. Gruden, CIPP/G
Counsel – Washington, D.C.
Phone: +1.202.624.2545
Email: mgruden@crowell.com