Cybersecurity & Government Contracts Update

November 2021

DoD Announces (New) CMMC 2.0

Key Notes:

- DoD announced CMMC 2.0, which is intended to streamline and clarify information security compliance obligations.
- CMMC 2.0 decreases the number of compliance "Levels" and allows for self-assessments for certain contractors.
- DoD will not impose any CMMC 2.0 requirements until future rulemaking is complete and it will suspend the current CMMC piloting efforts.
- A virtual CMMC 2.0 "Town Hall" is scheduled for November 9, 2021 to address its scope and changes.

The U.S. Department of Defense (DoD) recently announced significant changes to its Cybersecurity Maturity Model Certification (CMMC) program, which sets forth certain information security standards and processes applicable to defense contractors and subcontractors. The new "CMMC 2.0" is intended to address several issues and concerns raised by private industry as to the cost and complexity of the original program and is a product of a comprehensive internal assessment that DoD recently undertook. It will have a significant impact on all defense contractors, especially small businesses.

Background

In 2020, DoD amended the Defense Federal Acquisition Regulation Supplement (DFARS) to require defense contractors and subcontractors to submit cybersecurity assessments to the DoD prior to the award of a government contract and to implement and maintain technical, physical, and administrative security controls to protect and safeguard certain types of controlled unclassified information and other sensitive data and obtain third-party cybersecurity certification of these controls (i.e., "CMMC 1.0"). In particular, the original CMMC 1.0 program required contractors to comply with one of five different levels of security controls based on the types of information and data they collected and processed pursuant to a government contract or subcontract. For example, contractors subject to the CMMC 1.0 Level 1 standard had to comply with the basic safeguarding requirements set forth in FAR 52.204-21, and those subject to CMMC Level 5 had to comply with over 150 security requirements, practices, and processes.

CMMC 2.0 – What's New?

The new CMMC 2.0 program is intended to simplify and streamline compliance obligations. Most significantly, CMMC 2.0 will address the following:

- *NIST controls*. It relies on information security standards set forth by the National Institute of Standards and Technology (NIST), which are well established and common across industries.
- *Compliance levels*. It reduces the number of compliance "Levels" from five to three: (1) Foundational (e.g., requirements aligning to the basic security practices in FAR 52.204-21), (2) Advanced (e.g., requirements based on NIST SP 800-171), and (3) Expert (e.g., requirements based on NIST SP 800-172).
- *Assessments (and self-assessments)*. It permits companies associated with the new Level 1 (Foundational) and some Level 2 (Advanced) acquisition programs to perform self-assessments to demonstrate their compliance (instead of having to undergo a third-party security assessment). However, organizations

subject to Level 2 (Advanced) will be required to undertake triannual third-party assessments for critical national security information and may have to comply with an annual self-assessment for select programs. Level 3 (Expert) will be required to undertake triannual government-led assessments.

- *POA&MS and waivers*. It allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification and permits DoD to grant waivers to CMMC requirements under certain limited circumstances.

In addition, DoD indicated that it will increase oversight of the professional and ethical standards of third-party assessors, which will have a significant role in ensuring defense contractors are verifiably in compliance with the CMMC 2.0 security levels.

Next Steps and Additional Resources

DoD announced the changes in CMMC 2.0 will be implemented through the rulemaking process, which will have a notice and comment period. Importantly, DoD also stated that while these rulemaking efforts are ongoing, it will suspend the current CMMC piloting efforts and will not approve the inclusion of a CMMC requirement in any DoD solicitation. The interim rule for CMMC 1.0 had previously established a five-year phase-in period, during which CMMC compliance was only required in select pilot contracts. DoD stated that CMMC 2.0 will not be a contractual requirement until it completes rulemaking to implement the program and that the rulemaking process can take 9 to 24 months.

The changes to the CMMC are summarized on DoD's CMMC website and include FAQs. The CMMC Accreditation Body will discuss CMMC 2.0 during a virtual "Town Hall" on November 9 from 6:00-7:00 p.m. ET, which will be recorded and posted online after the event.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com

Joseph R. Berger
202.263.4193
Joseph.Berger@ThompsonHine.com

Tom Mason
202.263.4168
Thomas.Mason@ThompsonHine.com

Francis E. (Chip) Purcell, Jr.
202.263.4118
Chip.Purcell@ThompsonHine.com

or any member of our Privacy & Cybersecurity or Government Contracts groups.