Government Contracts and Privacy & Cybersecurity Update

September 2024

DOD Proposes Rule for Implementing Cybersecurity Maturity Model Certification 2.0 Program

Key Notes:

- DOD's proposed rule amends DFARS requirements in part to require contractors to demonstrate at the time of contract award compliance with the CMMC level mandated in the solicitation.
- The proposed rule also requires contractors to complete and maintain the affirmation of continuous compliance with security requirements on an annual basis or when changes occur and to notify the contracting officer of any changes or lapses in CMMC certification levels during performance.
- Comments on the proposed rule are due by October 15, 2024.

The Department of Defense (DOD) issued a proposed rule on August 16 addressing the agency's implementation of the Cybersecurity Maturity Model Certification (CMMC) 2.0 program, which requires contractors to adhere to cybersecurity standards to protect certain types of unclassified information through the defense supply chain.

As background, two categories of federal rules will govern the CMMC program: (i) the "comprehensive and scalable assessment mechanisms" underlying the creation of the CMMC program, which are subject to pending regulations issued December 26, 2023, and (ii) the rule proposed on August 16, 2024, addressing contract clauses to be included within defense contracts, which incorporate the CMMC program rule. Specifically, this more recent proposed rule imposes specific requirements on both agencies and contractors regarding CMMC compliance and creates a three-year timetable for implementation.

The proposed rule amends the DOD Federal Acquisition Regulation Supplement (DFARS) regulations, and it requires contractors to demonstrate at the time of contract award, either through a current CMMC certificate or self-assessment, compliance with the CMMC level mandated in the solicitation. Under the revised regulations, before awarding a contract or exercising an option, the agency must verify that the CMMC compliance results are posted in the Supplier Performance Risk System (SPRS) for each DOD unique identifier (UID) and that the apparently successful offeror affirms continuous compliance with the applicable security requirements.

The proposed rule includes a new DFARS clause that specifies that the agency must notify contractors of the CMMC level required by the solicitation. The DFARS clause also specifies the proof of CMMC compliance that the offeror must post in SPRS: (i) offerors must post CMMC Level 1 and 2 self-assessments in SPRS; (ii) third-party assessment organizations must post CMMC Level 2 certificate assessments in SPRS; and (iii) the DOD assessor must post CMMC Level 3 certificate in SPRS. The proposed rule further includes prescriptive DFARS language notifying apparently successful offerors that they will not be eligible for an award if they do not have the results of CMMC compliance posted in SPRS and do not affirm their continuous compliance with the applicable security requirements.

The proposed rule amends DFARS 252.204-7021, governing CMMC requirements, to several obligations upon contractors:

- Under the proposed rule, contractors must complete and maintain the affirmation of continuous compliance with security requirements annually or when security changes occur. Such affirmation must be made by a senior company official, as defined in the regulations.
- The proposed rule also mandates that contractors may only transmit data on information systems certified at the CMCC level required by the contract to process, store, or transmit controlled unclassified information (CUI) or federal contract information (FCI) during contract performance.
- Further, contractors must notify the contracting officer of any changes in the contractor information systems that process, store, or transmit CUI or FCI during contract performance.
- Contractors also must notify the contracting officer of any lapses or changes in CMMC certification levels that affect the requirements for information security during contract performance. It is unclear how the term "lapse" will be applied in practice, and it appears to be separate from the incident response requirements imposed on defense contractors outlined in other provisions within the DFARS.
- Contractors must include the requirements of DFARS 252.204-7021 in all subcontracts, including those for acquiring commercial products and services (but excluding commercially available off-the-shelf (COTS) items). Contractors also must ensure that covered subcontractors have the appropriate CMMC level prior to awarding a subcontract.

The proposed rule sets forth a phased roll-out process lasting three years following the issuance of the final rule. During the three-year phase-in period, the CMMC requirements would apply only to the extent a solicitation or contract requires a contractor to maintain a specified CMMC level. After the phase-in period, the CMMC requirements would apply to all contracts that require the contractor to process, transmit, or store CUI or FCI during performance.

Comments on the proposed rule are due by October 15, 2024.

FOR MORE INFORMATION

For more information, please contact:

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

Steven G. Stransky
216.566.5646
202.263.4126
Steven.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

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

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2024 THOMPSON HINE LLP. ALL RIGHTS RESERVED.