Kiteworks

COMPLIANCE BRIEF

48 CFR CMMC Proposed Rule Published; Moves CMMC Closer to Implementation

With Final Rule Published, Expectations Set for 3-year Timeline to See CMMC in DoD Contracts

The Department of Defense (DoD) proposed to amend the Defense Federal Acquisition Regulation Supplement (DFARS) through 48 CFR Parts 204, 212, 217, and 252 [Docket DARS-2020-0034], published on August 15, 2024. This proposed rule, known as DFARS Case 2019-D041, aims to incorporate contractual requirements related to the Cybersecurity Maturity Model Certification (CMMC) 2.0 program. The rule partially implements a framework for assessing contractor compliance with cybersecurity requirements and enhances the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Expected Scope and Timeline of CMMC Implementation

This regulation will apply to Defense Industrial Base (DIB) contractors and subcontractors who process, store, or transmit FCI or CUI. It covers all DoD solicitations and contracts above the micro-purchase threshold, except those exclusively for Commercial Off-The-Shelf (COTS) items. Key implications include the requirement for contractors to obtain and maintain specified CMMC levels, post results of CMMC self-assessments in the Supplier Performance Risk System (SPRS), provide annual affirmations of compliance, and flow down requirements to subcontractors. The implementation timeline spans three years after the final rule is published, following a 60-day public comment period. During the first three years, the rule will only affect contracts specifically requiring CMMC. From the fourth year onward, it will apply to all relevant DoD contracts. By year 4, the DoD estimates that 29,543 entities (69% being small businesses) will be affected.

Next Steps and Economic Impact of CMMC Compliance

For DIB organizations, immediate next steps include reviewing the proposed rule, preparing to submit comments within the 60-day period, assessing their current cybersecurity posture against CMMC levels, planning for future compliance and certification needs, and monitoring for the final rule publication and implementation timeline. While no immediate action is required with this publication, organizations should be well on their way to preparing for the eventual implementation of these new cybersecurity requirements within CMMC 2.0 or risk losing out on DoD contracts.

Solution Highlights

- FedRAMP Moderate Authorized
- 3PAO security assessments
- Immutable audit logs
- FIPS 140 compliant
- Granular policy controls

While specific costs for CMMC certifications and self-assessments are addressed in a separate 32 CFR rule, the financial impact is significant. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016, with a potential 10-year cost of $512 billion to $979 billion at a 2% discount rate.

Streamlining CMMC Compliance With Kiteworks' Comprehensive Solution

Kiteworks offers robust support for organizations seeking to comply with CMMC requirements and the new DFARS ruling. Kiteworks' Private Content Network is FedRAMP Moderate Authorized and supports nearly 90% of CMMC 2.0 Level 2 requirements out of the box, providing a comprehensive solution for protecting CUI and FCI. With features such as secure file sharing, email protection, managed file transfer, and web forms, Kiteworks creates a Private Content Network (PCN) that ensures the security of sensitive data. The platform's strong access controls, encryption capabilities, and audit logging functionalities align closely with CMMC requirements across multiple domains, including Access Control, Audit and Accountability, and System and Communications Protection. By leveraging Kiteworks, organizations can significantly streamline their CMMC compliance efforts, reduce the risk of data breaches, and are that much closer to maintaining the necessary security posture to compete for and work on DoD projects under the new DFARS regulations.

The publication of the 48 CFR CMMC proposed rule marks a significant step toward implementing comprehensive cybersecurity measures in the DIB. As organizations prepare for the three-year implementation timeline, the need for robust, compliant solutions becomes paramount. Kiteworks stands at the forefront of CMMC compliance support, offering a FedRAMP Moderate Authorized platform that supports nearly 90% of CMMC 2.0 Level 2 requirements out of the box. With its Private Content Network, strong access controls, double encryption capabilities, and comprehensive audit logging, Kiteworks provides a comprehensive approach to protecting CUI and FCI. As DIB contractors navigate the complexities of CMMC compliance, Kiteworks offers a streamlined path to support organizations working to meet the new DFARS regulations, reduce cybersecurity risks, and maintain competitiveness in DoD contracts.

Kiteworks