Kiteworks

COMPLIANCE BRIEF

CMMC 2.0 Rulemaking Procedure and the False Claims Act

What organizations doing business with the DoD need to know about CMMC 2.0 and how the False Claims Act is making noncompliance a costly decision

CMMC 2.0

Cybersecurity Maturity Model Certification (CMMC) 2.0 is a set of standards created by the Department of Defense (DoD) to increase the security of the country and minimize cyber threats to the supply chain. Achieving CMMC compliance is a requirement for organizations seeking to bid on DoD contracts, and the level of compliance required depends on the sensitivity of the information they will handle. Organizations doing business with the DoD must comply with these standards, or face fines and penalties under the False Claims Act.

CMMC 1.0 had five maturity levels, but CMMC 2.0 reduced them to three tiers and aligned closely to NIST 800 standards. Level 1 is foundational and requires annual self-assessment with attestation from a corporate executive. It consists of 17 basic cyber-hygiene practices that all companies in the defense supply chain must implement. Companies at this level must demonstrate that they have established basic security practices to protect federal contract information (FCI). Level 2 is mapped to NIST SP 800-171 and requires triennial third-party assessments from CMMC Third Party Assessor Organizations (C3PAOs) for contractors that send, share, receive, and store critical national security information. A total of 110 practices must be implemented at this level, which includes configuration management, incident response, identification and authentication, and maintenance. Level 3 is expert, aligned with NIST SP 800-172, and will require triennial government-led assessments. It is still in production and the specifics have not yet been made public.

Final Rulemaking Expectations

CMMC 2.0 updates the program structure and requirements, which will be implemented through rulemaking in both Title 32 and Title 48 of the Code of Federal Regulations via the Defense Federal Acquisition Regulation Supplement (DFARS) and to finalize the National Institute of Standards and Technology (NIST) 800-171 assessment methodology and requirements. Both rules are scheduled for release in May 2023. Changes to CMMC 2.0 include reducing the number of levels from five to three, removing maturity processes and unique practices from all levels, and requiring independent third-party assessments for prioritized acquisitions involving controlled unclassified information (CUI) at Level 2.

The DOD has previously stated that the rulemaking process may take up to 24 months to complete, although they have also said it could take 15 to 24 months to implement the changes through rulemaking. According to contracting attorney Robert Metzger, the likely 32 CFR rule will go out for public comment in summer 2023 as a proposed rule and be released as a final rule in 2024. It is pivotal for organizations to stay compliant with their contract if they claim to be implementing controls, as according to Metzger, “companies remain subject to the existing cyber contract requirements, and they can demonstrate their achieved security by having C3PAO assessments done before the rules are final.”

In the first comprehensive, independent study of the DIB's cybersecurity maturity, conducted by Merrill Research and commissioned by CyberSheath, "A shocking 87% of contractors have a sub-70 Supplier Performance Risk System (SPRS) score, the metric that shows how well a contractor meets Defense Federal Acquisition Regulation Supplement (DFARS) requirements." An organization can demonstrate their achieved security by having C3PAO assessments done before the rules are final. If organizations are not compliant, they are expected to disclose any breaches under the Civil Cyber Fraud Initiative.

Cost of Noncompliance

Compliance with CMMC 2.0 is critical to maintaining security in the supply chain and ensuring the protection of sensitive data. Noncompliance with CMMC 2.0 is not an option and could result in dire consequences for organizations doing business with the DoD. The Civil Cyber-Fraud Initiative, which combines the department's expertise in civil fraud enforcement, government procurement, and cybersecurity, uses the False Claims Act to pursue cybersecurity-related fraud by government contractors and grant recipients. This Act includes a whistleblower provision that allows private parties to assist the government in identifying fraudulent conduct and share in any recovery while being protected from retaliation. Failure to comply with CMMC 2.0 can lead to fines of $10,000 per control, with a minimum of 110 controls in Level 2, under the False Claims Act. Compliance with CMMC 2.0 is critical to maintaining supply chain security, protecting sensitive data, and preventing new and emerging cyber threats to the security of critical systems and information.

CMMC 2.0 is a crucial security standard that DoD contractors must adhere to when bidding on DoD contracts. CMMC 2.0 reduces the number of levels from five to three and requires independent third-party assessments for prioritized acquisitions involving CUI at Level 2. Organizations not complying with CMMC 2.0 may face fines of $10,000 per control under the False Claims Act. Compliance is critical to preventing new and emerging cyber threats to the security of critical systems and information, and failure to comply can lead to severe consequences.