Kiteworks

COMPLIANCE-BRIEFING

FÜR CISOS UND COMPLIANCE-VERANTWORTLICHE DER DIB

CMMC Phase II Ist Pausiert. Ihr Compliance-Risiko Nicht.

Warum Die Aussetzung Durch Das DoW Den Prüfzeitplan Ändert, Nicht Die Zugrunde Liegende Pflicht Zum Schutz Von CUI

CMMC 2.0 | DFARS 7012 | NIST SP 800-171 | FedRAMP

Die Herausforderung

Am 13. Juli 2026 setzte das Department of War die Anforderungen für Drittanbieter-Assessments der CMMC Phase II aus, die ursprünglich für den 10. November 2026 vorgesehen waren. Die Schlagzeilen lasen sich wie eine Entwarnung. Am Markt wurde das als Erlaubnis verstanden, Investitionen in die Cybersicherheit zurückzufahren. Beides ist unzutreffend: Die eigene Mitteilung des DoW stellt unmissverständlich klar, dass die Aussetzung 'die Pflicht der Unternehmen zum Schutz föderaler Daten nicht aufhebt', und dass Auftragnehmer unabhängig vom CMMC-Einführungszeitplan weiterhin an DFARS 252.204-7012 gebunden bleiben.

Die Lösung

Kiteworks unterstützt Auftragnehmer der Defense Industrial Base dabei, die Lücke zwischen dem, was sich auf dem Papier geändert hat, und dem, was sich in der Praxis nicht geändert hat, zu schließen. Die Plattform deckt von Haus aus 90 % der Anforderungen von CMMC 2.0 Level 2 ab, ist FedRAMP Moderate Authorized und FIPS 140-3-validiert. Damit können Auftragnehmer ihre tatsächliche Sicherheitslage durch Selbstbewertung und Audit-Protokollierung nachweisen, nicht nur auf dem Papier, während das DoW seine 60-tägige Programmüberprüfung durchführt.

Was die eigenen Zahlen des DoW zeigen

100.000+
DIB-Unternehmen, die weiterhin ein Drittanbieter-Assessment benötigen

~100
Derzeit verfügbare C3PAOs, um sie zu bewerten

60 Tage
Dauer der Reformprüfung, bevor Empfehlungen fällig sind

Warum Prüfungsbereitschaft Jetzt Weiterhin Zählt

Der Rückstand bei den Assessoren verschwindet nicht von selbst
Der CIO des DoW selbst nannte die rund 100.000 DIB-Unternehmen, die ein Assessment benötigen, gegenüber nur etwa 100 verfügbaren C3PAOs als Grund für die Pause. Dieser Engpass löst sich während einer 60-tägigen Prüfung nicht von selbst auf. Auftragnehmer, die sich jetzt prüfungsbereit machen, vermeiden es, sich später um denselben engen Kapazitätsengpass zu bewerben, sobald Phase II wieder aufgenommen wird.

DFARS 7012 wurde nie ausgesetzt
Die vertragliche Pflicht, geschützte Verteidigungsinformationen zu sichern, besteht unabhängig vom Einführungszeitplan der CMMC. Die Zugriffskontrollen, Verschlüsselung und Audit-Protokollierung von Kiteworks decken direkt die Sicherheitsbereiche ab, die DFARS 7012 und NIST SP 800-171 verlangen.

Selbstbewertung erhöht die Anforderungen an die Genauigkeit
Da Prüfungen durch Dritte pausiert sind, gibt es für selbst attestierte SPRS-Werte keine externe Kontrolle mehr, bevor man sich auf sie verlässt. Eine ungenaue Selbstbewertung kann weiterhin ein Risiko nach dem False Claims Act darstellen, weshalb eine dokumentierte, prüfungsbereite Plattform in dieser Übergangsphase wichtiger wird, nicht unwichtiger.

Warum Prüfungsbereitschaft Jetzt Weiterhin Zählt

Staatlich geführte Bewertungen laufen weiter
Das DoW bestätigte, dass es NIST SP 800-171 Rev 2 in der Übergangszeit weiterhin durch Selbstbewertungen und ausgewählte staatlich geführte Bewertungen durchsetzen wird, mit Schwerpunkt auf greifbarer Cyberhygiene statt administrativem Aufwand.

Weitergabepflichten setzen sich nicht zurück
Hauptauftragnehmer müssen Cybersicherheitsanforderungen weiterhin an Subunternehmer weitergeben, und laufende Ausschreibungen, die bereits CMMC Level 2 referenzieren, werden durch die Pause bei der Einführung nicht automatisch entlastet.

Phase II ist pausiert, nicht gestrichen
Eine CMMC Reform Task Force führt bereits eine öffentliche RFI mit einer 60-tägigen Frist durch. Die Erfahrung legt nahe, dass die Anforderung in irgendeiner Form zurückkehrt, möglicherweise schneller, sobald die Kapazität der Assessoren behoben ist. Abwarten verkürzt lediglich die verbleibende Zeit, um später konform zu sein.

Wo Kiteworks Heute Ansetzt

Unterstützung für 90 % von CMMC 2.0 Level 2
Konfigurationsmanagement, Zugriffskontrolle, Audit und Verantwortlichkeit sowie System- und Informationsintegritätskontrollen sind in die Plattform integriert.

Konsolidierter Audit-Trail
Ein einziges Echtzeit-Aktivitätsprotokoll über E-Mail, Dateifreigabe, Managed File Transfer und Webformulare, das direkt in SIEM-Systeme einfließt und so die Prüfungsbereitschaft sicherstellt.

FedRAMP High In Process
Kiteworks hat seine Sicherheitsfunktionen für die föderale Cloud erweitert und für seine Secure Gov Cloud den Status FedRAMP High In Process erreicht. Dieser Meilenstein baut auf dem etablierten FedRAMP Moderate Authorized Federal-Cloud-Dienst auf, der seit Juni 2017 ununterbrochen autorisiert ist.

FIPS-140-3-validierte Verschlüsselung
Doppelte Verschlüsselung im Ruhezustand und bei der Übertragung, wobei Kunden bei jedem Schritt die Kontrolle über ihre Verschlüsselungsschlüssel behalten.

Lassen Sie aus einer Papierkram-Pause keine Compliance-Lücke werden

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.