# New Report by Kiteworks and Coalfire Reveals Significant Gaps in CMMC 2.0 Preparedness Across Defense Industrial Base

*Less than half of DIB contractors ready for certification as compliance deadline approaches*

SAN MATEO, CA, UNITED STATES, March 26, 2025 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, and Coalfire, a global services and solutions company specializing in advisory, assessment, and cybersecurity, released today a comprehensive report titled "State of CMMC 2.0 Preparedness in the DIB," that reveals critical readiness gaps among defense contractors as they work toward Cybersecurity Maturity Model Certification (CMMC) 2.0 compliance.

> "These findings should serve as a wake-up call for the Defense Industrial Base."
> *Frank Balonis, CISO and SVP of Operations at Kiteworks*

The report findings indicate that despite approaching deadlines, a majority of Defense Industrial Base (DIB) contractors are significantly behind in their preparedness efforts. Only 46% of organizations surveyed reported being ready to seek CMMC 2.0 Level 2 certification, while 57% have yet to complete a thorough gap analysis against NIST SP 800-171 requirements. The report surveyed 209 senior leaders from DIB organizations—which was conducted by third-party survey provider Centiment—on their CMMC 2.0 Level 2 readiness.

"These findings should serve as a wake-up call for the Defense Industrial Base," said Frank Balonis, CISO and SVP of Operations at Kiteworks. "With nearly half of contractors lacking a detailed Plan of Action and Milestones to address compliance gaps, and over one-third operating without comprehensive policies for Controlled Unclassified Information protection, the DIB faces substantial cybersecurity vulnerabilities that put sensitive defense information at risk."

The report highlights several concerning trends:
- Only 44% of DIB contractors have implemented continuous monitoring for systems within the scope of CMMC 2.0 Level 2 compliance.
- Less than 53% have fully implemented required access control measures across all relevant systems.
- Over 30% lack advanced controls to ensure third parties can only access CUI to which they are authorized.

- More than 30% do not enforce multi-factor authentication across all systems processing or storing sensitive data.

Technical implementation challenges represent the greatest perceived obstacle to achieving compliance, cited by 44% of respondents, followed closely by budgetary and resource constraints at 43%.

“The complexity of CMMC 2.0 requirements is driving organizations to seek expert guidance, with nearly 80% of DIB contractors engaging third-party consultants, Registered Provider Organizations, or C3PAOs," said Tom McAndrew, CEO at Coalfire. "As an advisory services provider and an authorized C3PAO, we're witnessing firsthand how critical expert assessment and implementation guidance is for organizations navigating these complex requirements.”

While the compliance landscape appears challenging, the report also outlines pathways to accelerate readiness. Kiteworks' Private Content Network solution helps organizations satisfy up to 90% of the 110 controls required for CMMC 2.0 Level 2 certification, providing a comprehensive approach to securing sensitive defense information across communication channels. Meanwhile, Coalfire's C3PAO certification services offer the expert assessment and validation needed to achieve and maintain compliance.

“The path to CMMC 2.0 compliance doesn't need to be overwhelming,” added Balonis. “With the right technology solutions and expert guidance, DIB contractors can efficiently implement the necessary controls while strengthening their overall security posture against evolving threats.”

The full report, “State of CMMC 2.0 Preparedness in the DIB,” can be downloaded at https://www.kiteworks.com/cmmc-preparedness-dib-report.

Findings from the report will be discussed in-depth in a roundtable on April 2 at 10 AM PST | 1 PM EST featuring subject-matter experts from Kiteworks and Coalfire. Register to attend the roundtable.

About Kiteworks
Kiteworks’ mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications. Headquartered in Silicon Valley, Kiteworks protects over 100 million end users for over 35,000 global enterprises and government agencies.

About Coalfire
Coalfire, headquartered in Denver, Colorado, is a global services and solutions company

specializing in advisory, assessment, and cybersecurity. The company develops cutting-edge technology platforms that automate defenses against security threats for the world's leading enterprises, cloud providers, and SaaS companies. Coalfire is the foremost provider of FedRAMP compliance assessments and penetration testing services in the United States.

David Schutzman
Kiteworks
+1 203-550-8551
email us here
Visit us on social media:
Facebook
X
LinkedIn
YouTube

---