Kiteworks

TOP 5

Top 5 Reasons DIB Contractors Standardize CUI Governance on Kiteworks

How Enterprise Defense Contractors Unify CMMC 2.0 Compliance Across Business Units, Subsidiaries, and Supply Chain Partners

Large defense contractors do not face one CMMC problem—they face dozens, replicated across business units, subsidiaries, and supply chains that may include hundreds of subcontractors, each subject to flowdown. Phase 2 third-party assessments begin November 10, 2026, and primes are now contractually accountable for the CMMC posture of every vendor handling their CUI. Tool sprawl across email, file sharing, MFT, SFTP, and AI workflows has produced fragmented audit logs that cannot survive a C3PAO assessment. Kiteworks gives enterprise contractors a single CUI control plane—one policy engine, one audit log, one assessment boundary.

1 One CUI Control Plane Across Every Business Unit

Enterprise defense contractors typically run five or more disconnected systems handling CUI: Microsoft 365 in one division, a legacy SFTP appliance in another, an MFT product for engineering data, and ad hoc email for everything else. Each silo carries its own access controls, retention rules, and audit trail—a separate attack surface and a separate assessment scope. Kiteworks consolidates email, secure file sharing, MFT, SFTP, web forms, and APIs under a single Private Data Network with one policy engine, one immutable audit log, and one identity model federated across business units. Assessors examine one tamper-evident record covering AC, AU, and SC controls, not a reconstruction stitched across five separate products.

2 Coexists With Your Existing IAM, SIEM, and DLP Investments

Large contractors have spent years building enterprise IAM (Okta, Entra ID, Ping), SIEM (Splunk, Sentinel, QRadar), and DLP investments—and rip-and-replace is a non-starter. Kiteworks deploys as a single-tenant hardened virtual appliance that integrates with the stack you already operate: SAML and SCIM into your IAM, real-time syslog and CEF feeds into your SIEM, and DLP scanning that respects your existing Microsoft Purview or Forcepoint policies. CMMC Level 2 inherits from your existing controls instead of duplicating them. Your security team gets one more managed integration, not another standalone product to operate.

3 Demonstrate Supply Chain Flowdown to DoW Assessors

Under DFARS 252.204-7021, primes are accountable for ensuring CMMC compliance across every subcontractor that touches their CUI. The 2025 Kiteworks DIB survey found 62% of organizations lack adequate governance controls and 34% are immature on third-party CUI access. Kiteworks gives primes a defensible flowdown architecture: invite subcontractors into a shared CUI workspace where every file exchange is policy-enforced, fully audited, and tied to verified identities. When an assessor asks how you govern CUI flowing to subs, you produce one report covering the entire supply chain.

4 Continuous Monitoring Across Federated Business Units

A CMMC assessment is a point-in-time event, but defense programs run for years and business units drift between assessments. M&A activity inherits noncompliant environments. Engineering teams adopt new collaboration tools without telling security. The Kiteworks platform delivers continuous compliance monitoring across every business unit on the Private Data Network: real-time control dashboards, automated System Security Plan updates, and immediate alerting when a policy is bypassed. Your CISO walks into the next board meeting with evidence of continuous compliance, not a snapshot from 18 months ago.

5 Customer-Held Encryption Keys and FedRAMP High In Process

Enterprise contractors are increasingly asked—by DoW program offices, insurers, and their own boards—to prove no third party can compel access to CUI in their custody. Kiteworks customers retain sole encryption key custody: Neither Kiteworks, the cloud provider, nor law enforcement has access to the data. That structural sovereignty answers the custody questions raised by Microsoft's January 2025 disclosure of BitLocker recovery keys. Kiteworks has held FedRAMP Moderate Authorization since June 2017, with FedRAMP High In Process under active review.

www.kiteworks.com

June 2026