Kiteworks

CAPABILITIES BRIEF

FOR FEDERAL SECURITY AND PROCUREMENT TEAMS

"FedRAMP Equivalent" Is Not FedRAMP

How BOD 26-04 Converts a Marketing Claim Into an Operational Liability — and What Verified Authorization Actually Proves.

FedRAMP High In Process | FedRAMP Moderate Authorized | BOD 26-04

The Challenge

CISA's Binding Operational Directive 26-04, released June 10, 2026, requires Federal Civilian Executive Branch agencies to remediate critical Known Exploited Vulnerabilities within three days when public exposure, KEV catalog listing, automatable exploitation, and full system control converge. Managed file transfer and secure data exchange platforms have repeatedly appeared in the KEV catalog. Yet many agencies run platforms that describe themselves as "FedRAMP equivalent" — a self-attested marketing claim with no 3PAO review, no Authority to Operate, and no continuous monitoring package. When a KEV entry activates BOD 26-04 timelines, those agencies have no independent way to verify their vendor patched in time. "FedRAMP equivalent" is not a security posture — it is a marketing decision.

The Kiteworks Difference

Kiteworks is FedRAMP High In Process, with Coalfire Systems' 3PAO assessment complete and the package under active federal agency sponsor review. Kiteworks has also maintained FedRAMP Moderate Authorization continuously since 2017 — assessed annually across 325 NIST SP 800-53 controls with FIPS 140-3 validation. Monthly vulnerability scans, annual penetration test results, and an open Plan of Action and Milestones (POA&M) are submitted to Kiteworks' authorizing official, not assembled in response to a procurement inquiry. FedRAMP authorization requires four independently verified steps that no vendor can self-certify — equivalency requires none of them.

Continuous Authorization by the Numbers

2017
FedRAMP Moderate Authorization Since

325
NIST SP 800-53 Controls Assessed Annually

3 Days
BOD 26-04 Patch Window for Critical KEVs

What FedRAMP Authorization Actually Requires

3PAO Assessment

An accredited Third Party Assessment Organization evaluates controls against the FedRAMP Moderate baseline. No self-assessment qualifies.

Authority to Operate

A federal authorizing official independently reviews findings and formally accepts risk by issuing an ATO. No vendor can issue its own.

Continuous Monitoring

Monthly vulnerability scans, annual pen tests, and an open POA&M — an ongoing requirement, not a one-time badge.

Marketplace Listing

Status appears on fedramp.gov/marketplace. If a vendor's listing shows no active status, they are not FedRAMP authorized.

FedRAMP "Equivalent" vs. FedRAMP Authorized (Kiteworks)

FedRAMP "Equivalent"

A self-attested marketing claim with none of the independent verification federal buyers require.

- ✓ No accredited 3PAO assessment
- ✓ No Authority to Operate issued
- ✓ No continuous monitoring package
- ✓ Patch status is vendor self-reported
- ✓ Cannot fulfill BOD 26-04 documentation requirement
- ✓ Not listed on fedramp.gov/marketplace

FedRAMP Authorized (Kiteworks)

Independently verified authorization federal agencies can confirm today.

- ✓ Annual 3PAO assessment by Coalfire Systems
- ✓ ATO issued by federal authorizing official
- ✓ Monthly vulnerability scans submitted to AO
- ✓ Open POA&M with independently reviewed timelines
- ✓ Documentation exists before an agency inquiry
- ✓ Listed and verifiable at fedramp.gov/marketplace

Three Steps That Change the Outcome

1 VERIFY FIRST

Check the FedRAMP Marketplace Before Any Vendor Conversation

Search fedramp.gov/marketplace by vendor name before any pricing discussion — no active listing means no FedRAMP authorization, and no documentation changes that fact.

2 ASK THREE QUESTIONS

Require Documentation for Any Equivalency Claim

Name the 3PAO. Provide the SSP, SAP, SAR, and open POA&M. Demonstrate DFARS 252.204-7012 compliance — no documentation, no standard.

3 REQUIRE COMMITMENT

Demand a Patch Velocity Commitment Before Signing

Ask how the vendor will notify you of a KEV and prove patch completion within the BOD window — equivalency vendors have no independent mechanism, just self-reported status.

The Kiteworks Control Plane for Secure Data Exchange

FedRAMP High In Process

Coalfire's 3PAO assessment is complete; the package is under active federal sponsor review.

FedRAMP Moderate Authorized

Authorized since 2017; assessed annually across 325 NIST 800-53 controls; FIPS 140-3 validated.

Audit-Ready at All Times

The monitoring package already exists, reviewed before any agency inquiry.

Continuous Monitoring Built In

Monthly scans, annual pen tests, and an open POA&M — submitted to an AO, not assembled on demand.

CUI and Zero Trust Aligned

Aligns with zero trust and CUI obligations in ways a self-assessment cannot replicate.

Unified Secure Channels

Consolidates email, file sharing, managed file transfer, and web forms into one monitored environment.

Is Your Agency Running a Verified Platform or a Marketing Claim?

Verify Kiteworks Authorization

- Search "Kiteworks" at fedramp.gov/marketplace to confirm current authorization status
- Request Kiteworks' continuous monitoring package as part of procurement due diligence
- Ask about the FedRAMP High In Process trajectory and its federal sponsor review
- Contact Kiteworks Public Sector at kiteworks.com/federal for your agency's BOD 26-04 posture

Talk to Kiteworks Public Sector About Your BOD 26-04 Posture

www.kiteworks.com/federal

Copyright © 2026 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.