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.

BOD 26-04 | FedRAMP Authorized | Continuous Monitoring

The Challenge

CISA's Binding Operational Directive 26-04, released June 10, 2026, requires Federal Civilian Executive Branch (FCEB) agencies to remediate critical Known Exploited Vulnerabilities (KEVs) within three days when four risk factors converge: public exposure, KEV catalog listing, automatable exploitation, and full system control on success. Managed file transfer and secure content exchange platforms — the exact infrastructure agencies use to move sensitive data with contractors and partners — have repeatedly appeared in the KEV catalog. Yet many agencies are running platforms that describe themselves as "FedRAMP equivalent," a self-attested marketing claim with no Third Party Assessment Organization (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 mechanism to verify their vendor patched in time.

The Kiteworks Difference

Kiteworks has maintained FedRAMP Moderate Authorization continuously since June 2017 — assessed annually by Coalfire Systems, an accredited 3PAO, across 325 NIST SP 800-53 controls with FIPS 140-3 validation. Monthly vulnerability scanning reports, 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. When a KEV entry lands, the documentation already exists. For agencies with higher-impact data requirements, Kiteworks is FedRAMP High In Process, with Coalfire's 3PAO assessment complete and FedRAMP PMO review underway.

Continuous Authorization by the Numbers

2017
FedRAMP Moderate Authorization First Granted

325
NIST SP 800-53 Controls Assessed Annually

3 Days
BOD 26-04 Patch Window for Critical KEVs

What "Equivalent" Actually Means

"FedRAMP equivalent" is not a security posture — it is a marketing decision. FedRAMP authorization requires four independently verified steps that no vendor can self-certify. Equivalency requires none of them. BOD 26-04 has compressed the timeline between winning a contract on an equivalency claim and being exposed by it when KEV patch timelines activate.

What FedRAMP Authorization Actually Requires

3PAO Assessment

An accredited Third Party Assessment Organization evaluates the vendor's controls against the FedRAMP Moderate baseline. No self-assessment qualifies — a 3PAO must be accredited by the FedRAMP PMO.

Authority to Operate

A federal authorizing official independently reviews the 3PAO's findings and formally accepts the risk by issuing an ATO. No vendor can issue their own ATO.

Continuous Monitoring

Monthly vulnerability scans, annual penetration tests, and an open POA&M submitted to the authorizing official — an ongoing operational requirement, not a one-time badge.

Marketplace Listing

Authorized status appears on marketplace.fedramp.gov where any agency can verify it directly. If the vendor is not listed as Authorized, they are not FedRAMP authorized.

FedRAMP "Equivalent"

Self-attested security posture with no independent verification and no standing on the FedRAMP Marketplace.

✓	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 marketplace.fedramp.gov

FedRAMP Authorized (Kiteworks)

Independently verified, continuously monitored authorization — the same security infrastructure BOD 26-04 compliance requires.

✓	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 marketplace.fedramp.gov

Three Steps That Change the Outcome

1 VERIFY FIRST

Check the FedRAMP Marketplace Before Any Vendor Conversation

Go to marketplace.fedramp.gov and search by vendor name before opening a feature comparison or pricing discussion. Every cloud service with Authorized status is listed there. If the vendor isn't under Authorized, they are not FedRAMP authorized — no amount of documentation changes that fact. Five minutes at the start of due diligence answers the question that matters most.

2 ASK THREE QUESTIONS

Require Documentation for Any Equivalency Claim

Ask every vendor: (1) Have you been assessed by a FedRAMP-recognized 3PAO — and can you name them? (2) Can you provide the full body of evidence: SSP, SAP, SAR, and open POA&M? (3) Can you demonstrate compliance with DFARS 252.204-7012 for cyber incident reporting, malware, media preservation, and forensic access? A vendor who cannot answer all three affirmatively — with documentation — is not operating at the standard that matters under BOD 26-04.

3 REQUIRE COMMITMENT

Demand a Patch Velocity Commitment Before Signing

Ask prospective vendors: "How will you notify us when a KEV entry affects your platform, and how will you demonstrate patch completion within the BOD timeline?" For FedRAMP-authorized vendors, the answer is documented in the continuous monitoring package. For equivalency-claiming vendors, there is no independent mechanism — just self-reported patch status with no external verification.

The Kiteworks Control Plane for Secure Data Exchange

FedRAMP Moderate Authorized

Continuously authorized since June 2017, assessed annually by Coalfire Systems across 325 NIST SP 800-53 controls. FIPS 140-3 validated. FedRAMP High In Process.

Continuous Monitoring Built In

Monthly vulnerability scans, annual penetration testing, and open POA&M management are operational requirements — submitted to an authorizing official, not assembled on demand.

Unified Secure Channels

Consolidates email, file sharing, managed file transfer, and web forms into a single, continuously monitored environment — every channel through which agencies exchange sensitive data with contractors and partners.

Audit-Ready at All Times

When a KEV entry forces the BOD 26-04 documentation question, the continuous monitoring package already exists — reviewed by an independent authorizing official before any agency inquiry.

CUI and Zero Trust Aligned

FedRAMP's continuous monitoring requirements align with zero trust architecture and CUI handling obligations in ways a point-in-time self-assessment cannot replicate.

FedRAMP High In Process

Coalfire's 3PAO assessment is complete and FedRAMP PMO review is underway — signaling the same continuous investment in independent verification that Moderate authorization already proves.

> Platforms that have completed FedRAMP Moderate authorization maintain the continuous monitoring infrastructure BOD 26-04 compliance requires. The monthly scans, annual penetration test, and open POA&M are not assembled in response to an agency inquiry. They exist because authorization requires them.
>
> **Frank Balonis**
> CISO and SVP of Operations, Kiteworks

Verify Kiteworks Authorization

- Search "Kiteworks" at marketplace.fedramp.gov to confirm Authorized status before any vendor conversation
- Request Kiteworks' continuous monitoring package — monthly vulnerability scans, annual pen test, and open POA&M — as part of procurement due diligence
- Ask about the FedRAMP High In Process trajectory: Coalfire assessment complete, FedRAMP PMO review underway
- Contact Kiteworks Public Sector at kiteworks.com/federal to discuss your agency's BOD 26-04 compliance posture

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

www.kiteworks.com/federal