dispersive

SOLUTION BRIEF · FEDERAL PQC MANDATES

Meet Federal PQC Mandates on Schedule, Without Rip-and-Replace

Dispersive® Stealth Networking delivers post-quantum cryptography, crypto agility and Harvest Now, Decrypt Later (HNDL) mitigation on the communications it carries, built on a FIPS 140-3 validated cryptographic module.

Executive Summary

Federal policy has put hard dates on replacing cryptography, and the coming acquisition rule carries them down the supply chain. Two problems sit inside those dates: adversaries are collecting encrypted traffic today for decryption later, and AI-accelerated cryptanalysis can overturn a scheme's assumptions faster than an estate can be re-engineered. Dispersive answers both.

Data cited in Citi Institute's quantum-threat research puts the risk on a near-term timeline, not a distant one. Prediction-market data cited by Citi in January 2026 put the odds of a useful quantum computer at roughly 8% before 2027 and about 39% before 2030, the same year federal key establishment must move to PQC. Citi also cites a 19–34% probability of widespread quantum breaking of public-key encryption by 2034. The same research is explicit about the cost of waiting: post-quantum cryptography protects what is transmitted after migration, not what was collected before it. A single-day quantum attack on one top-five U.S. bank's Fedwire access could put an estimated $2.0–$3.3 trillion in GDP at risk.

Which Mandates Apply to Which Organizations

Executive Order 14412 directs the FAR Council to propose a rule carrying post-quantum obligations into federal contracts, with a proposed rule due around December 19, 2026. An organization with no direct federal contract can inherit the requirement by selling to a company that holds one, and agencies writing migration plans are already asking vendors about cryptographic posture. Regulated commercial firms are moving as well, pressing for PQC planning ahead of any hard requirement, and institutions are building migration programs to protect customer and stakeholder trust.

If you are	What is required	Key dates
A federal civilian agency	Migrate high-value assets and high-impact systems to NIST-standardized PQC. Submit a migration plan, keep a cryptographic inventory, name a PQC migration lead.	Migration plans due in 2026. Key establishment by December 31, 2030. Signatures by December 31, 2031.
An NSS or defense program	Support the CNSA 2.0 suite in new acquisitions: AES-256 for data in transit, ML-KEM-1024 for key establishment and ML-DSA-87 for signatures, under CNSSP 15 and the DoW PQC Strategy.	New acquisitions compliant from January 1, 2027. DoW systems support PQC by December 31, 2030 and use PQC by December 31, 2031.
A federal prime contractor	Comply with NIST FIPS incorporating the finalized post-quantum algorithms. The obligation arrives through FAR rulemaking directed by EO 14412.	Proposed rule expected around December 19, 2026. Compliance targeted for December 31, 2030.
A subcontractor or supplier	The same obligations, flowed down through prime contracts. No direct federal contract is needed to inherit the requirement.	Follows the prime contract schedule, anchored on December 31, 2030.

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

Three PQC Mandate Realities Are Network Problems

Each one shows up on the paths your data travels while systems are being migrated. Data in motion is vulnerable at the transport layer. Here is how Dispersive protects it.

01 · EXECUTIVE ORDER 14412

"…the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum computers are operational."

They can't break what they can't capture.

Harvest depends on capturing whole conversations. Dispersive splits each session into independently encrypted segments across paths that keep moving, so a collector on any one link captures fragments, and reassembly requires collecting across several paths at once while preserving their timing. It addresses the half of quantum risk that algorithm replacement does not.

Multipath splitting · Automated Moving Target Defense · Costlier collection

02 · FEDERAL PQC STRATEGY

"Mission capability and capacity should not be sacrificed during the migration."

Keep data moving while crypto is replaced.

Migration happens in stages: encryptors re-keyed, endpoints and terminals refreshed, gateways re-platformed, each on its own schedule. Dispersive spreads every session across the paths still in service and shifts traffic automatically, so a link taken down for upgrade does not end the mission thread.

Multipath session splitting · Automatic path failover · Transport-agnostic

03 · FEDERAL PQC STRATEGY

"Nearly every deployed asset will be affected in some way…"

Resilience without another system to migrate.

Dispersive is a lightweight overlay on transport already in place, replacing none of the endpoints, appliances or encryptors on your migration plan. Because it operates at the transport layer, algorithm change happens in one place rather than inside every application.

Lightweight overlay · Crypto agility in one place · No rip-and-replace

Excerpted from Executive Order 14412 (91 FR 38483) and federal post-quantum cryptography strategy guidance. Reference to these documents does not imply U.S. Government endorsement. Reference to Citi Institute research does not imply endorsement.

One Deployment Solves Three Requirements

Most PQC programs solve one problem at a time: migrate the algorithms, then prove agility, then worry about what was collected in the meantime. Dispersive delivers all three on the paths it carries, without displacing anything already in place.

Requirement	What Dispersive delivers
Post-quantum cryptography	NIST-standardized ML-KEM and ML-DSA across the data plane and the control plane, on FIPS 140-3 validated cryptographic modules. Headers and payloads use separate AES-256 keys, so compromising one does not expose the other. AES-256 is the symmetric algorithm specified in CNSA 2.0, so together this covers all three parts of the CNSA 2.0 core: key establishment, signatures and data transport. Traffic carried over Dispersive is post-quantum protected from the day it is deployed.
Crypto agility	Algorithms change in one place rather than inside every application, appliance and endpoint. This is the requirement agencies and contractors find hardest to evidence, and the one that determines the cost of every transition after this one.
Harvest Now, Decrypt Later mitigation	Each session is split into independently encrypted segments across paths that keep changing, so a collector on any one link captures fragments rather than conversations. This is the half of quantum risk that algorithm migration does not reach.

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

Dispersive Accelerates PQC Compliance

Dispersive installs as a lightweight overlay, as DispersiveCloud® managed service or DispersiveFabric™ on premises. That makes it a practical insertion point: no rip and replace, and none of the endpoints, appliances or encryptors on your migration plan touched. The communications it carries are post-quantum protected on NIST-standardized ML-KEM and ML-DSA from the day it is deployed. Keep the encryption you already run. Dispersive encapsulates existing traffic inside its post-quantum protected transport, so nothing in your environment changes. Add Dispersive, and the communications it carries gain post-quantum protection, crypto agility and HNDL mitigation the day it is deployed.

Your highest-consequence paths are protected while the rest of the estate is still being inventoried. Your crypto agility requirement has a working answer rather than a plan. And the vendor readiness response we supply goes straight into your third-party coordination record.

Dispersive provides a network-layer control that supports and accelerates compliance for the communications it carries. Multipath segmentation and moving paths make collection and reconstruction materially harder, particularly from a single observation point. Inventory, applications, endpoints, identities, signatures, stored data, governance, and third-party coordination remain part of the broader program.



© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

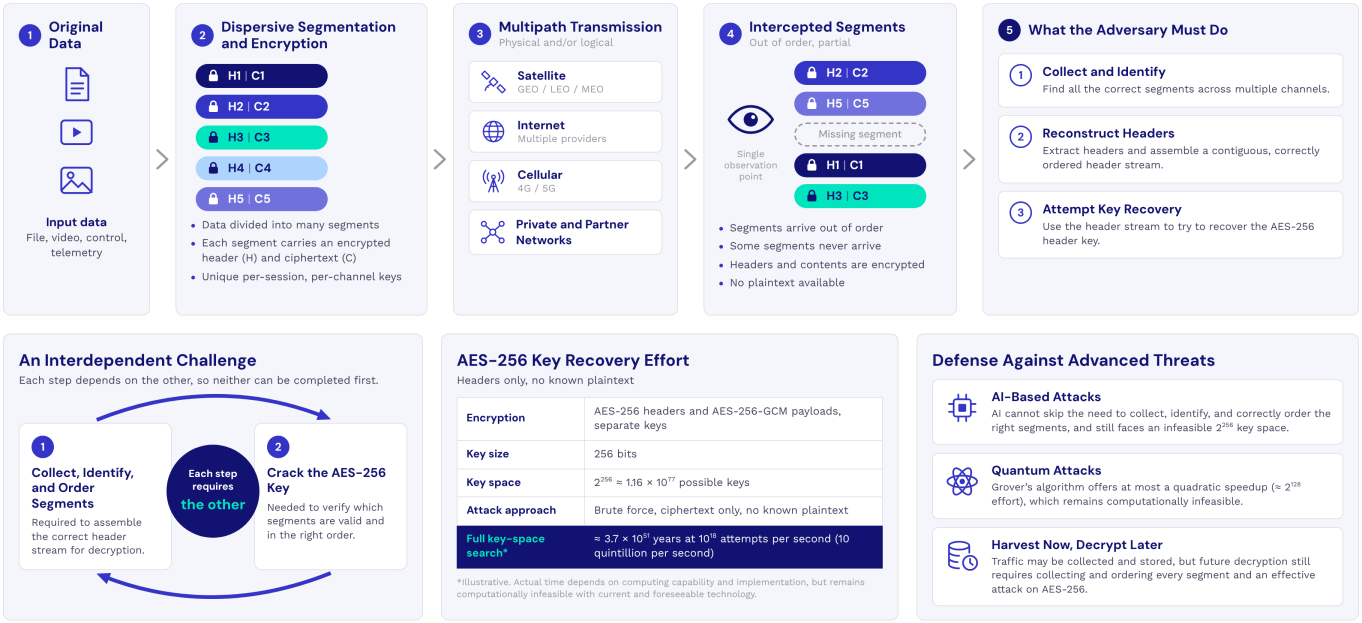
Harvest Now, Decrypt Later

The adversary is already on the network. Salt Typhoon reached inside major U.S. telecommunications carriers, and Volt Typhoon has been prepositioned in U.S. critical infrastructure. Sensitive data has a long tail, so harvest now, decrypt later is today's collection and tomorrow's breach. On a conventional encrypted tunnel the full session travels one predictable path, and a single vantage point captures all of it.

Dispersive moves the problem from mathematics to collection. A quantum computer or a frontier AI model attacks the math. Neither puts a collector on every path at once. Headers are encrypted as well as payloads, so a collector cannot pick out the segments that belong to a given conversation. To attempt to break Dispersive, an adversary must collect every segment on every path, reconstruct the encrypted headers in the correct order, and only then attempt to recover the header key. Identifying the right segments and their order depends on that same key. This does not address endpoint compromise, key compromise, or data already at rest.

What an Adversary Must Do to Attempt to Crack Dispersive® Stealth Networking

An interdependent collection, identification, and decryption challenge



Crypto Agility Is an Immediate Requirement

AI is accelerating cryptanalysis, and it may reach some cryptography before quantum computers do. A Financial Times report (28 October 2026) found that AI advances could break some core encryption methods, including some newer quantum-resistant algorithms, before quantum computing becomes a comparable threat. The Wall Street Journal (6 November 2026) reported that cryptographers are now debating whether AI-driven mathematics will reach encryption first. In July 2026, Anthropic's Frontier Red Team reported that a researcher working with Claude Mythos Preview cut the effective key size of HAWK, a post-quantum signature candidate, in half in roughly sixty hours. HAWK has since been withdrawn.

The standards held. ML-KEM and ML-DSA were unaffected. But quantum threatens today's public-key math and AI may erode confidence in its replacements, so agility decides whether the next break is a configuration change or a re-engineering program.

Sources: Financial Times, "AI maths advances raise fears over security of global encryption," 28 October 2026; The Wall Street Journal, "Quantum Computers Are Poised to Crack Encryption. AI Could Beat Them to It," 6 November 2026. References do not imply endorsement.

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io

Credentials

THE DISPERSIVE OVERLAY

- Lightweight software overlay: multipath session splitting and Automated Moving Target Defense (AMTD)
- Operates at the transport layer, so algorithm change happens in one place rather than inside every application
- DispersiveFabric™ on-premises, DispersiveCloud® as a managed option
- Deploys in minutes, with no disruption to existing VPN, ZTNA or SD-WAN investments

CRYPTOGRAPHY AND COMPLIANCE

- Post-quantum cryptography across the data plane and control plane, using NIST-standardized ML-KEM and ML-DSA
- Separate AES-256 keys for headers and payloads, so compromising one does not expose the other
- FIPS 140-3 Validated Cryptographic Module #5247; SOC 2 Type II and HIPAA certified
- DARPA-origin research heritage; 53 granted patents
- ECCN 5D002 under EAR, not ITAR

Validated FIPS 140-3 cryptography. FIPS 140-2 certificates moved to historical status in September 2026, and agencies are directed not to use historical modules in new procurements. The cryptographic module powering Dispersive services is FIPS 140-3 validated under CMVP certificate #5247, which primes and suppliers can cite directly, including in CMMC Level 2 assessments.

The Federal PQC Calendar

The dates are fixed. Between them, systems are re-keyed, refreshed and replaced in stages, and the network must keep carrying the traffic.

Nov 2025
Agency CIO memo
PQC migration leads named; cryptography inventoried

Jun 2026
EO 14412 · DoW PQC Strategy
Federal deadlines set, FAR rule directed

2026
Migration plans due
OMB M-26-15: civilian agencies submit PQC plans

Dec 2026
Proposed FAR rule
Contractor PQC compliance rule, due approx. Dec 19

1 Jan 2027
CNSA 2.0 · NSS gate
New NSS acquisitions compliant by default
Risk marker: about 8% odds of a useful quantum computer before 2027

31 Dec 2030
Support or phase out
Key establishment on PQC; contractors meet PQC FIPS
Risk marker: about 39% odds of a useful quantum computer before 2030

Civilian agency milestones apply to non-national security systems. National Security Systems follow the CNSA 2.0 timeline under CNSSP 15.

Accelerate PQC Compliance with Dispersive

01
Identify the critical use cases, data flows and assets that require post-quantum protection or compliance.

02
Contact Dispersive to assess your highest-consequence communications paths and current cryptographic dependencies.

03
Receive a migration blueprint for immediate post-quantum protection, crypto agility and HNDL mitigation, without changing your network or providers.

Dispersive Holdings, Inc.
300 Colonial Center Pkwy Suite 100
Roswell, GA 30076 USA | dispersive.io | 1.844.403.5850

dispersive

© 2026 Dispersive Holdings, Inc. | All Rights Reserved | dispersive.io