WP-041
24 June 2026
14 sections

US FEDERAL POST-QUANTUM CRYPTOGRAPHY & EXECUTIVE POLICY

US Federal PQC Migration: Reading the June 2026 Executive Order on Advanced Cryptographic Attacks

On 22 June 2026 the White House ordered federal agencies to move high value assets and high impact systems to NIST post-quantum standards. Key establishment by 2030. Digital signatures by 2031. The standards are published. The inventory work is not.

AffixIO Research | 24 June 2026 | Download PDF | Primary source: White House executive order

Expertise and sources

AffixIO Research · Cardiff and Swansea, UK. Post-quantum attestation, zero-knowledge verification, and Merkle audit infrastructure in production at affix-io.com/sandbox.

This paper reads the 22 June 2026 executive order against NIST PQC standards, FIPS 203/204/205, and AffixIO's published field reports. Patent pending GB2510622.0. AffixIO is not a US federal contractor and does not hold FedRAMP authorisation at the time of writing.

Published 24 June 2026 · Last reviewed 24 June 2026

EXECUTIVE SUMMARY

On 22 June 2026 President Trump signed *Securing the Nation Against Advanced Cryptographic Attacks*, an executive order that gives federal post-quantum cryptography migration the force of presidential policy. The order names OMB and the National Cyber Director as coordination leads, requires NIST and CISA to publish technical guidance, sets December 2030 as the deadline for post-quantum key establishment on high value assets and high impact systems, and December 2031 for digital signatures. It directs the FAR Council to propose rules requiring covered contractors to adopt NIST FIPS with PQC algorithms by 2030, and CISA to define minimum elements for a cryptographic bill of materials.

NIST finalised ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) in August 2024. Hybrid TLS deployments with X25519MLKEM768 are already measurable on the public internet. What the executive order adds is procurement leverage, agency accountability, and a defined role for critical infrastructure sector risk management agencies. What it does not solve is the full stack: channel encryption migration leaves long-lived audit records, identity verification stores, and eligibility databases as separate harvest-now-decrypt-later targets unless agencies treat attestation and verification as first-class migration workstreams.

This paper reads each substantive section of the order, maps obligations to NIST timelines, and states honestly where AffixIO fits: as verification and audit-layer infrastructure that complements TLS and PKI migration, not as a replacement for FIPS 140-3 validated encryption modules or agency HSM programmes.

Related research

- WP-036: Live PQC API sandbox field report
- WP-029: TLS 1.3 hybrid post-quantum deployment

- WP-019: Post-quantum PKI migration
- WP-033: PQC and zero-knowledge convergence
- WP-032: Sublinear post-quantum attestation

CONTENTS

AFFIXIO : PROVIDER PROFILE

AffixIO in the Federal PQC Stack

Federal PQC migration spans several layers: bulk encryption and key exchange in protocols, digital signatures on certificates and documents, validated cryptographic modules, procurement rules for contractors, and sector guidance for critical infrastructure. AffixIO operates at the **verification and audit attestation layer**. We do not sell HSMs, operate a federal PKI, or provide FIPS 140-3 validated bulk encryption modules. We provide post-quantum-

signed Merkle audit roots, zero-knowledge proof verification, and reproducible sandbox evidence that agency teams and integrators can inspect without trusting vendor logs alone.

Where AffixIO sits relative to the executive order

LAYER	EXECUTIVE ORDER FOCUS	TYPICAL PROVIDERS
Channel encryption	PQC key establishment on HVAs and high impact systems by 31 Dec 2030; TLS, VPN, session protocols	Cloud platforms, network vendors, OpenSSL/BoringSSL integrators
Digital signatures & PKI	PQC signatures on HVAs and high impact systems by 31 Dec 2031; code signing, document signing, certificates	PKI vendors, certificate authorities, platform signing services
Validated modules	CMVP acceleration within 180 days; FIPS 140-3 approved modes for PQC algorithms	HSM vendors, module labs, NSS programme for national security systems
Inventory & CBOM	Agency cryptographic inventory; CISA CBOM guidance within 270 days; automated algorithm assessment	Asset discovery vendors, SBOM/CBOM tooling, GRC platforms
Audit & verification attestation *← AffixIO*	ML-DSA-65 Merkle root signing on audit batches; ZK verification without harvestable identity stores; inclusion proofs for inspector and IG review; complements Sec. 5(d) CBOM by attesting what algorithms ran at verification time	**AffixIO : verification infrastructure**
Procurement &	FAR rules for covered contractors by 2030;	Prime contractors, FedRAMP CSPs,

contractors	VDPs covering cryptographic vulnerabilities	integrators subject to proposed FAR amendments

Capabilities relevant to federal programmes

ML-DSA-65 audit anchoring

One post-quantum signature on a Merkle root covers large audit batches. Aligns with FIPS 204 direction for long-lived integrity records that must survive quantum adversaries. Documented in WP-002 and live in the sandbox.

Stateless ZK verification

Prove eligibility or policy compliance without storing decryptable identity databases. Reduces harvest-now-decrypt-later exposure on verification stores that sit outside TLS scope. See WP-030.

Reproducible sandbox evidence

Public field report (WP-036) with latency tables and Merkle inclusion checks. Useful for pilot evaluations before procurement, not a substitute for ATO or FedRAMP.

Circuit-level algorithm disclosure

Open Noir circuit catalogue documents which verification paths run in production. Supports CBOM-style transparency for the verification layer without claiming full-stack CBOM coverage.

MCP and integrator tooling

Hosted MCP connector for prove/verify workflows from approved agent environments. Relevant to contractor innovation pilots, not mandated by the order.

Critical infrastructure adjacency

Sector SRMAs must assist owners and operators with PQC migration plans. AffixIO's IoT provenance and edge verification papers address attestation patterns CISA may reference for operational technology contexts.

> Honest scope note: AffixIO is a UK company. We serve integrators and programmes evaluating verification architecture. We do not claim current placement on GSA schedules, FedRAMP authorisation, or NSS approval. Federal adoption would require appropriate contracting vehicles, data residency decisions, and security assessment paths chosen by the agency.

SECTION 01

What changed on 22 June 2026

Post-quantum cryptography has been on federal roadmaps since NIST began its standardisation project in 2016. NIST released the first three final PQC standards in August 2024. NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) set expectations for national security systems. Industry moved hybrid TLS forward. Until June 2026, however, civilian agency migration remained largely guidance-driven rather than deadline-driven at cabinet level.

The executive order Securing the Nation Against Advanced Cryptographic Attacks changes that posture. Section 1 states policy explicitly: safeguard national security and maintain technological leadership by executing transition of federal information systems to NIST-approved FIPS for post-quantum cryptography, and assist critical infrastructure owners and operators with their transitions.

Three features distinguish this order from earlier memoranda:

- **Named coordination.** OMB and the National Cyber Director lead strategic oversight. NIST supplies technical guidance with NSA and CISA input. Responsibilities are assigned, not implied.
- **Scoped deadlines on the highest-risk systems.** High value assets and high impact systems must adopt PQC for key establishment by 31 December 2030 and digital signatures by 31 December 2031.

- **Procurement extension.** The FAR Council must propose contractor compliance rules, accelerating PQC adoption in the supply chain that agencies depend on.

The order does not declare a quantum computer exists today. It treats large-scale quantum capability in adversary hands as a credible future threat and ongoing collection against encrypted traffic as a present risk. That framing matches how security teams already model harvest-now-decrypt-later attacks.

SECTION 02

Deadlines and agency obligations

Section 4 of the order sets the operational calendar federal CIOs and PQC migration leads will track against.

WHEN	WHO	REQUIREMENT
Within 30 days	Each agency head	Identify PQC migration lead; report name and contact to OMB and National Cyber Director
Within 90 days	OMB (with CISA, National Cyber Director)	Issue guidance requiring agency inventory review, migration plans, and PQC transitions on HVAs and high impact systems
Within 180 days	NIST	Initiate internal PQC migration pilot; complete by 31 December 2027
Within 180 days	NIST	Revise CMVP processes to accelerate PQC module validations where appropriate
Within 180 days	FAR Council	Publish proposed rule: covered contractors comply with NIST FIPS including PQC by 31 December 2030
Within 270 days	CISA (with NIST)	Release public guidance on minimum elements for a cryptographic bill of materials
Within 270 days	FAR Council	Proposed rule on contractor VDPs including cryptographic vulnerability reports
31 December 2030	Agencies	PQC key establishment on all HVAs and high impact systems (excluding NSS)
31 December 2031	Agencies	PQC digital signatures on all HVAs and high impact systems (excluding NSS)
Annually until complete	NSA as National Manager for NSS	Report PQC migration status for national security systems

Section 6(a) adds a cost-coordination mandate: OMB, DoD, NASA, and GSA should identify shared procurement, cloud migration, training, and centralised technical support opportunities. Agencies under budget pressure should read that as permission to pool pilots rather than duplicate incompatible inventories.

2030

2031

Deadline for post-quantum key establishment on federal HVAs and high impact systems

Deadline for post-quantum digital signatures on the same system classes

SECTION 03

Definitions: HVA, high impact, migration lead

Section 2 definitions determine scope. Three terms will dominate agency planning documents.

HIGH VALUE ASSET (HVA)

Federal information or a federal information system designated under OMB Memorandum M-19-03 or successor policy. HVAs are already subject to enhanced cybersecurity scrutiny. The order adds explicit PQC transition requirements on top of existing HVA programme obligations.

HIGH IMPACT SYSTEM

An information system where at least one security objective (confidentiality, integrity, or availability) is assigned a FIPS 199 high impact rating. This is broader than the HVA label in some agencies and narrower in others. Inventory reconciliation between HVA lists and FIPS 199 categorisations is week-one work for the PQC migration lead.

PQC MIGRATION LEAD

An agency employee or detailee reporting to the CIO, responsible for cryptographic inventory management, prioritised migration planning, and cross-agency coordination. This role is the single accountable contact OMB and the National Cyber Director will expect on status reviews.

National Security Systems are explicitly carved out of the civilian agency deadlines in Section 4(b). NSA reports separately under Section 5(c). Civilian agencies should not assume NSS timelines apply to their systems, and NSS

programmes should not wait for civilian OMB guidance to define their own migration posture under CNSA 2.0.

SECTION 04

NIST standards and crypto-agility

The order defines PQC as cryptographic algorithms or methods designed to resist attack by both quantum and classical computers, and requires transition to NIST-approved FIPS. In production terms that means the August 2024 standards:

STANDARD	ALGORITHM	PRIMARY USE	EXECUTIVE ORDER DEADLINE
FIPS 203	ML-KEM (formerly CRYSTALS-Kyber)	Key establishment, TLS hybrid handshakes, VPN key exchange	2030 (key establishment)
FIPS 204	ML-DSA (formerly CRYSTALS-Dilithium)	Digital signatures, code signing, document attestation	2031 (digital signatures)
FIPS 205	SLH-DSA (formerly SPHINCS+)	Hash-based signatures; conservative fallback where lattice assumptions are unacceptable	2031 (digital signatures)

NIST IR 8547 describes a longer deprecation arc for quantum-vulnerable algorithms, with disallowance targeted by 2035 for many use cases. The executive order front-loads risk on HVAs and high impact systems. Agencies should not read 2035 as the planning horizon for sensitive systems.

Crypto-agility in practice

Crypto-agility means the ability to swap algorithms without rewriting entire applications. The order's CMVP acceleration directive acknowledges a practical constraint: validated modules lag reference implementations. OpenSSL 3.x with liboqs supports ML-KEM in many environments before a FIPS 140-3 validated module lists PQC in approved mode. Agencies will need risk acceptance documentation for interim deployments, exactly as NIST and industry guidance already recommends for hybrid TLS.

AffixIO uses ML-DSA-65 (the NIST Level 3 parameter set aligned with FIPS 204 family algorithms) for Merkle root signing on audit batches. That is an attestation choice on integrity records, not a claim that our hosted sandbox constitutes a FIPS 140-3 validated module for agency bulk encryption.

SECTION 05

Harvest now, decrypt later

Section 1 background text references adversaries collecting United States information now and decrypting it later once large-scale quantum computers are operational. This is harvest-now-decrypt-later (HNDL): store ciphertext today, break it when quantum resources become available.

HNDL shapes prioritisation. Data with decades-long sensitivity (classified derivatives, health records, intelligence sources, long-term financial contracts, infrastructure designs) needs PQC protection on the wire *and* on stored artefacts signed or encrypted under RSA, ECDSA, or ECDH today. It also applies to verification architectures that store enough identity material to reconstruct privileged access after a future break.

TLS migration addresses traffic in transit. It does not automatically re-sign ten years of archived audit logs, rotate every code-signing certificate in a supply chain, or eliminate centralised eligibility databases that hold attributes an adversary could decrypt later. Those are separate workstreams the order implies through inventory and signature deadlines but does not spell out per archive type.

Post-quantum attestation on Merkle roots, as described in WP-032, is one response for long-lived integrity records: sign today's audit batch roots with ML-DSA so a future quantum adversary cannot forge retroactive history even if they eventually break legacy signatures on older archives.

SECTION 06

Cryptographic inventory and CBOM

You cannot migrate what you cannot find. Section 4(b)(i) requires agencies to review inventories of HVAs and high impact systems. Section 5(d) directs CISA, coordinating with NIST, to publish minimum elements for a **cryptographic bill of materials** (CBOM) within 270 days.

A CBOM differs from a software bill of materials. Where an SBOM lists packages and versions, a CBOM lists cryptographic assets: algorithms (RSA-2048, ECDSA P-256, AES-256-GCM), protocol versions (TLS 1.2 vs 1.3), certificate authorities, key lengths, and where keys live (HSM, software keystore, cloud KMS). The goal is automated assessment, not a PDF attestation.

Minimum inventory fields agencies should track now

- System identifier and FIPS 199 impact level
- HVA designation (yes/no) and HVA programme ID if applicable
- Key establishment algorithms and protocol endpoints
- Signature algorithms on certificates, code, and documents
- Key custody model and rotation schedule
- Dependencies on contractor-hosted cryptography
- Planned PQC target algorithms (ML-KEM parameter set, ML-DSA parameter set, SLH-DSA variant)
- Validation status (FIPS 140-3 module, interim hybrid, risk-accepted pilot)

AffixIO's open circuit catalogue and API responses document algorithms used on the verification path (for example ML-DSA-65 on attestations, Groth16 or Noir backends on ZK proofs). That supports CBOM completeness for the verification layer when agencies integrate our APIs. It does not inventory cryptography inside unrelated agency applications.

SECTION 07

Two migrations: keys and signatures

The order treats key establishment and digital signatures as separate deadlines one year apart. That split is technically correct and operationally difficult.

Key establishment (31 December 2030)

Covers ML-KEM and hybrid key exchange in TLS 1.3, VPNs, secure messaging, and API session protection. Hybrid modes (classical plus PQC) are the de facto transition path documented in WP-029. X25519MLKEM768 is already observable on a large fraction of public TLS 1.3 handshakes. Federal agencies should prefer configurations that can be demonstrated in CBOM and network monitoring tools, not merely enabled on a staging load balancer.

Digital signatures (31 December 2031)

Covers ML-DSA and SLH-DSA replacing RSA and ECDSA on certificates, firmware signatures, document signing, and software supply chains. Signature migration is often slower because certificate chains embed trust anchors, timestamping services, and cross-organisational dependencies. ML-DSA signatures are larger than ECDSA (roughly kilobyte scale versus tens of bytes), which affects bandwidth, HSM storage, and embedded systems.

> Contractor deadline alignment: Section 6(c) targets covered contractor FIPS compliance including PQC by 31 December 2030, one year before the agency signature deadline. Contractors supplying key establishment and signing components may need to lead agency timelines, not follow them.

Verification infrastructure sits primarily on the signature side: post-quantum binding on audit roots, proof transcripts, and attestation objects. Session encryption for API calls to a verification service still follows the key-establishment migration path.

SECTION 08

FAR, contractors, and vulnerability disclosure

Section 6(c) and 6(d) extend migration beyond agency data centres into the federal supply chain.

Proposed FAR rule on PQC FIPS (6(c))

The FAR Council must publish a proposed rule within 180 days requiring covered contractors to comply with NIST FIPS incorporating PQC compliant algorithms by 31 December 2030. Proposed rules require notice and comment. The deadline is still meaningful for contract drafting today: agencies issuing multi-year integrator awards in 2026 should include flow-down language on PQC roadmaps even before the final rule lands.

Vulnerability disclosure programmes (6(d))

A second proposed rule must ensure covered contractors implement vulnerability disclosure policies consistent with NIST guidelines, and that those VDPs accept reports of cryptographic vulnerabilities, including testing for missing encryption and use of non-FIPS-approved algorithms. This connects PQC migration to the existing federal push on coordinated disclosure. Security researchers will have explicit standing to report weak or legacy cryptography in contractor systems.

For integrators evaluating AffixIO: our public security page and contact path support responsible disclosure. We do not claim compliance with every future FAR clause until the final rule text and agency supplements are published.

SECTION 09

CISA and critical infrastructure

Section 5(a) requires Sector Risk Management Agencies, as defined under National Security Memorandum 22 (April 2024) on critical infrastructure security and resilience, to work with CISA on PQC migration plans for owners and operators. Section 3(b) assigns NIST and CISA ongoing technical guidance duties.

Critical infrastructure operators face the same HNDL logic as federal agencies, often without OMB enforcement leverage. SRMA facilitation is how the order reaches energy, water, healthcare, and transportation networks that will not read FAR supplements but still depend on RSA and ECC in SCADA, medical devices, and payment terminals.

Section 5(b) tasks the State Department with engaging foreign governments and industry groups on NIST-standardised PQC, aligning international partners with US algorithm choices rather than fragmented national schemes.

AffixIO's IoT supply chain provenance paper (WP-028) addresses device authenticity attestation patterns relevant to operational technology contexts. We do not operate as an SRMA or CISA-designated provider. We publish architectures integrators can map to sector-specific control frameworks.

SECTION 10

Where TLS and PKI migration stops

Most public PQC guidance in 2026 focuses on TLS and PKI. That is necessary and incomplete.

After agencies deploy hybrid TLS and begin ML-DSA certificate pilots, several classes of system remain vulnerable or unverifiable:

- **Centralised eligibility and identity stores** that hold attributes attackers want to harvest
- **Mutable audit logs** that cannot demonstrate integrity to an inspector without trusting the log operator

- **Offline verification** at edge gates, clinics, or field offices without live HSM connectivity
- **AI and automated decision pipelines** where the compliance question is what was decided, not only how bytes were encrypted in transit

WP-033 names this the verification gap: PQC secures the channel, zero-knowledge proofs protect the claim, and neither alone closes the audit-layer harvest threat. The executive order's inventory and signature mandates create the policy hook for agencies to fund that gap as part of the same programme office handling TLS, not as an unrelated science project.

SECTION 11

Verification infrastructure for federal use

Mapping AffixIO capabilities to federal needs requires discipline. The following table states what we provide today in production APIs and the sandbox, and what agencies would still need from other suppliers.

FEDERAL NEED	AFFIXIO CONTRIBUTION	NOT PROVIDED BY AFFIXIO
PQC key establishment on agency TLS	Reference architectures in WP-029; no managed TLS termination	FIPS-validated network encryption appliances
PQC certificates and PKI	ML-DSA-65 on audit objects, not X.509 CA services	Agency PKI, FedPKI bridge integration
Cryptographic inventory	Algorithm disclosure on verification API paths	Enterprise-wide CBOM discovery agents
Long-lived audit integrity	Merkle batches with ML-DSA-65 root signatures; inclusion proofs	Agency records management policy
Privacy-preserving eligibility checks	ZK circuits for yes/no and threshold proofs without PII export	Authoritative identity issuers (state DMVs, federal credential services)
Inspector-verifiable evidence	Third parties can verify Merkle inclusion and signatures without AffixIO log access	Legal admissibility determinations per agency counsel
Contractor reproducibility	Public sandbox and MCP connector for structured pilots	FedRAMP ATO on behalf of the agency

Federal programmes that align with this model include: benefits eligibility verification where statute requires proof without over-collection; fraud prevention with tamper-evident decision records; supply chain integrity for devices touching critical infrastructure; and AI governance where OMB M-24-10 style accountability expects demonstrable safeguards at decision time.

SECTION 12

Pilot pathways and reproducible evidence

Section 4(c) requires NIST to run an internal PQC migration pilot by 31 December 2027. Agencies need not wait for NIST to finish before scoping their own pilots, but NIST's pilot will set a visible benchmark.

AffixIO recommends a reproducibility-first evaluation path aligned with how our existing field reports are written:

1. Read WP-036 and open the sandbox with no sales call required.
2. Run identity verify and one ZK circuit; capture `merkle_validation` JSON from responses.
3. Independently fetch the Merkle root from the documented API and verify inclusion proofs using published hashes.
4. Map observed algorithms to draft CBOM fields for the verification integration only.
5. Document risk acceptance gaps (hosting location, FedRAMP, data residency) before any production pilot on real citizen data.

Partnership pilots with scan-to-prove flows are documented in WP-039. That pattern fits integrators building sector-specific demos for SRMA outreach without exporting source data.

NIST's CMVP acceleration matters for pilots that require validated modules. Until PQC appears in approved FIPS 140-3 modes, agencies should document interim hybrid deployments explicitly in migration plans, as the order anticipates through NIST's process revision mandate.

SECTION 13

What AffixIO does not claim

Credibility on federal topics requires explicit limits.

- AffixIO is not a US government entity and does not speak for OMB, NIST, CISA, or the National Cyber Director.

- We are not currently FedRAMP authorised. Production federal use requires agency-specific risk decisions and appropriate contracting paths.
- Our hosted APIs are not a substitute for FIPS 140-3 validated modules where statute or policy mandates validated cryptography for bulk encryption.
- We do not provide complete CBOM or enterprise discovery across an agency fleet.
- Zero-knowledge proofs reduce data exposure; they do not replace legal authority to run a programme or conduct law enforcement.
- Patent pending GB2510622.0 covers aspects of our attestation architecture. Standard interoperability remains a design goal via open circuits and documented APIs.

If a programme needs only TLS hybrid deployment, AffixIO is not the first vendor to call. If a programme must show that decisions were made correctly, with post-quantum integrity on audit evidence and minimal harvestable identity state, our papers and sandbox are written for that evaluation.

SECTION 14

Conclusion

The June 2026 executive order makes federal post-quantum migration a cabinet-level programme with dates, roles, and procurement teeth. NIST standards give agencies algorithm choices. CMVP reform and FAR rules address the validation and supply-chain bottlenecks that slowed earlier transitions.

The remaining work is inventory, prioritisation, and honest accounting for systems TLS does not fully protect: long-lived records, verification stores, and attestations that must remain trustworthy under harvest-now-decrypt-later assumptions. AffixIO sits in that layer: post-quantum-signed audit roots, stateless verification, and reproducible public evidence. We complement the encryption migration the order mandates. We do not replace it.

Agency PQC migration leads should name verification and attestation workstreams in their 90-day plans, not only TLS and PKI. Contractors should prepare algorithm roadmaps before the FAR comment period closes. Critical infrastructure integrators should engage SRMA facilitation early. The order creates the policy frame. The engineering starts in the inventory spreadsheet.

> Primary source: Securing the Nation Against Advanced Cryptographic Attacks (The White House, 22 June 2026). NIST PQC standards: CSRC Post-Quantum Cryptography.

FREQUENTLY ASKED

US Federal PQC Executive Order: Common Questions

What deadlines does the order set?

31 December 2030 for post-quantum key establishment on high value assets and high impact systems. 31 December 2031 for post-quantum digital signatures on the same classes. Covered contractors face a 2030 FIPS compliance target under proposed FAR rules.

Which NIST algorithms are in scope?

ML-KEM (FIPS 203) for key establishment, ML-DSA (FIPS 204) for primary digital signatures, and SLH-DSA (FIPS 205) where hash-based signatures are preferred. Agencies should follow NIST and CISA guidance as it is updated after OMB's 90-day directive.

What is a cryptographic bill of materials?

An inventory format for cryptographic assets in software and hardware, enabling automated detection of legacy algorithms. CISA must publish minimum element guidance within 270 days of the order.

Where does AffixIO fit in US government architecture?

At the verification and audit attestation layer: ML-DSA Merkle anchoring, zero-knowledge proof verification, and reproducible sandbox evidence. Not at the bulk encryption, PKI, or FedRAMP authorisation layers unless future programmes place us there through normal contracting.

WP-036: Live PQC Sandbox | WP-029: Hybrid TLS | WP-033: PQC + ZK

Evaluate Docs Trust Center Security Status Whitepapers Contact

verification infrastructure | yes | no | proof