Preparing for Cybersecurity Risks in the Post-Quantum Era

FTI Consulting | Davis Wright Tremaine

Webinar | October 29, 2026

FTI CONSULTING | CYBERSECURITY

Davis Wright Tremaine LLP

Introductions



Michael Borgia

Partner

Davis Wright Tremaine

Mike Borgia leads DWT's Information Security practice, advising clients on cybersecurity, data privacy, and incident response. Mike is a trusted advisor to companies operating in many sectors, including telecommunications, financial services, cloud computing, information technology, and government contracting. He regularly advises on compliance with generally applicable and sector-specific information security and data privacy laws and frameworks in the United States and abroad.



Ankur Sheth

Senior Managing Director, Cybersecurity, Privacy, & AI

FTI Consulting

Ankur Sheth is a senior cybersecurity and data privacy leader with more than 25 years of experience helping organizations strengthen cyber resilience. He specializes in cybersecurity strategy, risk management, and technology implementation, guiding clients from assessment and program design through execution. Ankur works closely with executives, boards, and technology leaders to build and mature cybersecurity programs that enhance security posture and address evolving threats.



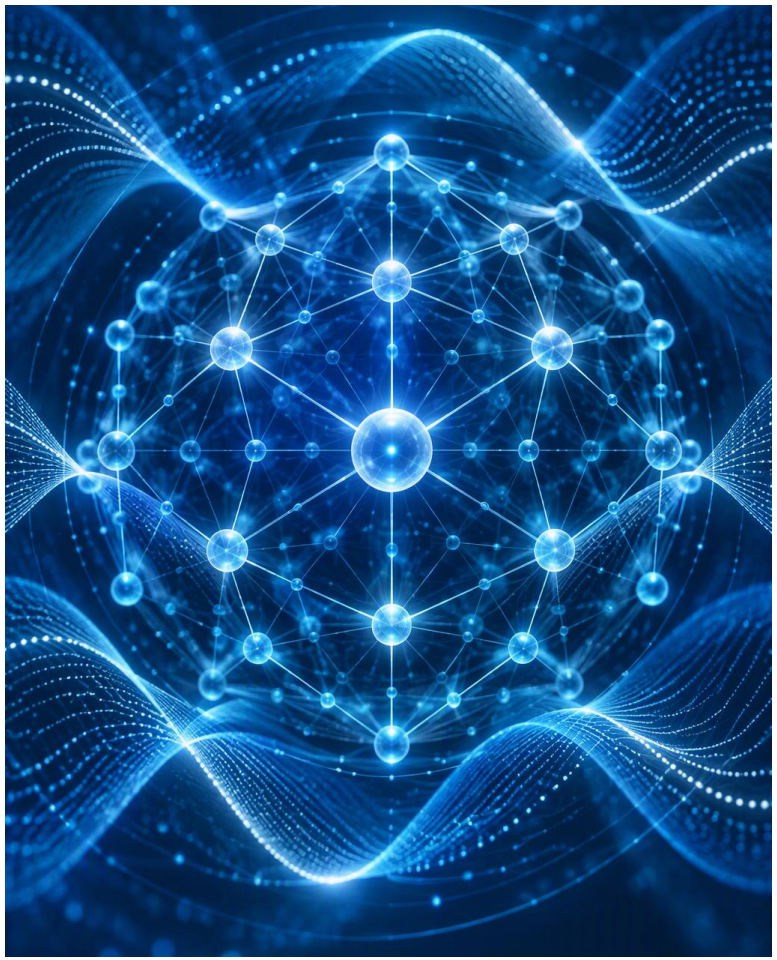
Greg Berkin

Senior Cybersecurity Advisor – Quantum AI

FTI Consulting

Greg Berkin is a Senior Advisor in FTI Consulting's Cybersecurity practice and a Fellow at Stanford's Center for Responsible Quantum Technology. With more than 30 years of experience as a technology executive, entrepreneur, and computer scientist, he advises clients on complex cybersecurity, quantum technology, and enterprise investigations. His expertise spans ransomware, network intrusions, spyware, cryptocurrency scams, data vulnerabilities, and technology-related litigation support.

Today's agenda



01 Overview and Background

Quantum basics, opportunities, and cybersecurity risks

02 Legal Framework

Legal and regulatory context for quantum readiness

03 FTI's Readiness Domains

A review of the eight domains, with deeper attention to cryptography, suppliers, and migration

04 Practical Responses

Critical systems, accountability, provider oversight and an audience checklist

Overview and Background

Quantum & Cryptography 101

Quantum computing poses significant risks to the **security of cryptography**, with the ability to potentially put entire infrastructures, networks, and applications at risk for widespread threats.

- Current public-key cryptography is expected to be broken by a large-scale quantum computer as soon as **three to eight years**.
- The quantum threat will **increase** data breaches of sensitive health and financial personal data, challenge the integrity of digital documents, and break certain cryptocurrency encryption.
- Although quantum computers bring fatal threats to asymmetric cryptography, such as **RSA**, they do not pose a fatal threat to symmetric cryptography, such as **AES** and **OTP**.



ars TECHNICA

Denny's THE ORIGINAL GRAND SLAM

In a first, cryptographic keys protecting SSH connections stolen in new attack

Dan Goodin • 11/13/2023 12:30 pm • Biz & IT, Features, Security

View non-AMP version at arstechnica.com

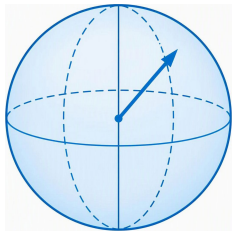
Computing

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

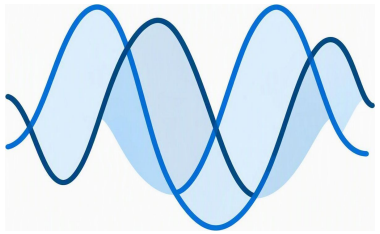
Quantum computing: the basics

Quantum computing uses the physics of very small particles to process information in new ways. It could solve certain problems much faster than conventional computers.



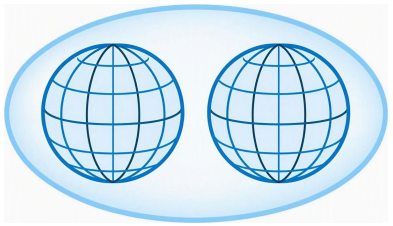
Qubit (quantum bit)

The basic unit of quantum information, which gives a 0 or 1 when measured.



Superposition

A qubit can hold a combination of the 0 and 1 states before measurement.



Quantum entanglement

Qubits can share a joint state, linking their measurement results even when separated.

Classical computers

Bits (0 or 1) and conventional logic power everyday tasks such as email, spreadsheets and business applications.

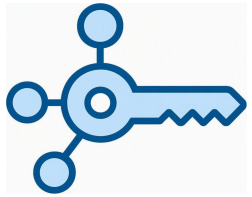
Quantum computers

Qubits and quantum operations may help with specific tasks, such as simulating molecules. Today's machines remain error-prone.

Quantum computers will complement classical computers. They will not make every task faster.

Public-key cryptography: the basics

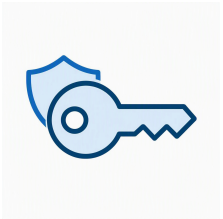
A way to protect information and prove who sent it using two mathematically linked keys: one public and one private.



PUBLIC KEY

Share it openly.

Others use it to encrypt or verify signatures.



PRIVATE KEY

Keep it secret.

The owner uses it to decrypt or create signatures.

Everyday uses

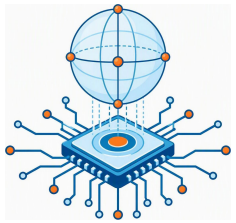
Secure connections

Websites, banking apps and VPNs establish shared keys for private communication.

Digital signatures

Verify who signed a message or software update and whether it changed.

The quantum threat



1. RSA and elliptic-curve methods rely on math that ordinary computers find hard to reverse.
2. A sufficiently powerful quantum computer could use Shor's algorithm to derive the private key from the public key (asymmetric).
3. **Exposed private keys could reveal data or enable forged signatures.**

Harvest now, decrypt later makes long-lived data a current concern

HOW HNDL WORKS



Collect today

An adversary captures encrypted traffic or copies protected information.



Retain over time

The adversary stores the material while computing capabilities develop.



Decrypt in the future

Vulnerable cryptography may eventually expose information that still matters.

Long secrecy lifetimes and long migration lead times increase the urgency to prepare.

Legal Framework

Federal PQC Transition: Executive Order 14412

Securing the Nation Against Advanced Cryptographic Attacks

2026

AGENCIES

Migration plans due to OMB (Oct.)

FAR COUNCIL

Proposed contractor rule due (Dec.)

2030

AGENCIES

Quantum-safe key establishment, high-value systems

CONTRACTORS

Meet PQC-compliant FIPS by Dec. 31

2031

AGENCIES

Quantum-safe digital signatures, high-value systems

2035

AGENCIES

All remaining federal systems migrated

CRITICAL INFRASTRUCTURE

SRMAs and CISA help owners and operators develop migration plans. No direct mandate.

By March 2027: CISA and NIST must release public guidance on the minimum elements of a "cryptographic bill of materials" (CBOM).

Related: Executive Order 14413

Ushering in the Next Frontier of Quantum Innovation

PQC Transition: The Broader Framework

Federal civilian systems

QCCPA
2022 statute
Inventory systems; OMB directs migration

→

EOs 14144 / 14306
2025
PQC adoption. 14306 amends 14144.

→

EO 14412
2026
Sets the 2030–2031 clock

→

OMB M-26-15
2026
The playbook: phases and agency plans

→

FAR Rule
proposed ~Dec. 2026
Extends reqs. to contractors

National security systems

CNSSP-15 + NSA's CNSA 2.0 (and FAQs)
Required algorithms and dates for national security systems. New acquisitions to be CNSA 2.0 compliant (or upgradable) by **January 1, 2027.**

NSM-10 (2022): Set the original 2035 goal and started the inventories. EO 14412 accelerates the timeline for high-value systems.

FIPS 203–205 (2024) NIST's post-quantum standards
203: ML-KEM for key establishment. 204: ML-DSA and 205: SLH-DSA for digital signatures.

No law expressly requires PQC (yet), but exposure still exists.



Board oversight (Caremark)

Directors and officers have a duty of loyalty to oversee “mission-critical” risks, including cybersecurity. Boards must be briefed and must be aware of legal requirements and industry standards.



FTC Section 5 and state UDAP laws

“Reasonable security” evolves with industry standards. PQC adoption will accelerate in the next few years.



Securities and Exchange Commission (SEC)

Risk management and governance disclosures; risk factor disclosures.

SWITZERLAND · FINMA, JULY 2026

Existing governance and risk rules already cover quantum risk. PQC roadmap expected by mid-2027.

Existing Laws Already Address Quantum Risks

GLBA Safeguards Rule

Written risk assessment and encryption of customer information in transit and at rest

NYDFS Part 500

Risk assessment, encryption, and asset inventory. **Sept. 2026 guidance: assessments must cover quantum computing.**

Encryption safe harbors

Most state breach laws exempt encrypted data unless the key is compromised.

Harvested today

Encrypted: no notice

Decrypted tomorrow

Notice? When does the clock start?

Readiness Domains

FTI's Readiness Domains

1 Governance & Strategy

Accountability, risk appetite and funding for a sustained transition.

2 Cryptographic Inventory

Where cryptography operates, what it protects and who owns it.

3 HNDL Risk

Long-lived information whose exposure could matter after future decryption.

4 Crypto Agility

The ability to change algorithms and keys without redesigning every service.

5 PQC Migration Readiness

A feasible sequence of pilots, upgrades and validated cutovers.

6 Third-Party & Supply Chain

Supplier dependencies, product support and evidence of readiness.

7 OT & Embedded Systems

Long-lived devices, limited update paths and operational constraints.

8 Awareness, Training & IR

Skills and response plans for cryptographic incidents.

Domain 2: the inventory must support decisions

Cryptographic Inventory

What the record needs

Business service and technical owner

- Data classification and secrecy lifetime
- Algorithm, key size and protocol
- Certificate, library and hardware dependencies
- Provider, version and support end date
- Evidence source and last verified date

How to find and use it

Combine application and network discovery with certificate, key-management and supplier records.

- Trace each critical service across internal and external dependencies.
- Prioritize vulnerable public-key use, long-lived data and difficult replacements.

The standards cover key establishment and signatures

PQC runs on conventional computing infrastructure

The approved building blocks

FIPS 203: ML-KEM

- Establishes a shared secret for use with symmetric encryption.

FIPS 204: ML-DSA

- Provides digital signatures.

FIPS 205: SLH-DSA

- Provides hash-based digital signatures.

What approval does not prove

An algorithm standard does not certify an entire product or deployment.

- Check protocol support, implementation assurance and interoperability.
- Test key and signature sizes, latency, certificate handling and recovery.
- Choose hybrid designs only where the applicable guidance and protocol support them.

Domain 5: migration readiness requires a workable cutover plan

PQC Migration Readiness: preparation



Prioritized scope

Rank services by data lifetime, business impact and the difficulty of changing them.



Architecture and dependencies

Agree on target protocols, key handling and vendor prerequisites before scheduling changes.



Funded delivery plan

Assign service owners and budget for testing, implementation and legacy replacement.

PQC Migration Readiness: delivery

Pilot acceptance

Test compatibility, performance and security against explicit criteria.



Controlled cutover

Use change approval, monitoring and a tested rollback that records residual risk.



Evidence of closure

Verify the production configuration, remove obsolete paths and update the inventory.



Domain 6: supplier readiness must match the service

Third-Party & Supply Chain

Where dependencies hide

Cloud and SaaS transport security

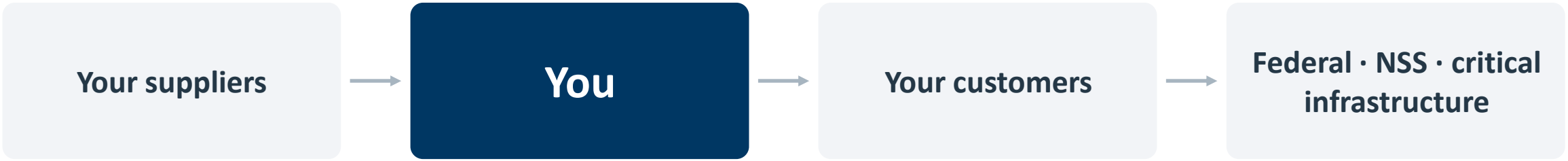
- Identity platforms and certificate authorities
- Network equipment, VPNs and HSMs
- Software libraries and update signing
- Managed services and subcontractors
- Embedded products with long support lives

Evidence worth requesting

Supported algorithms and protocol versions

- Product-level availability dates
- Customer configuration responsibilities
- Interoperability and performance results
- Subsupplier dependencies and exclusions
- Upgrade costs, support terms and fallback options

Domain 6: know where you sit in the supply chain



Your supply chain

- Which vendors hold your long-lived data or keys?
- Their cryptography is your exposure
- What contractual rights do you have? What obligation do suppliers have?
- Build PQC into due diligence and renewals

Supply chains you're part of

- Your software in a federal offering? FAR flow-downs will reach you
- Selling into NSS? Take note of CNSA 2.0 dates.
- Customers' deadlines become your contract terms

Provider fit is a delivery question

Proposed questions before accepting a supplier roadmap

Pace

- Will supported releases arrive before your critical-service deadlines?

Coverage

- Does the plan cover your products, interfaces, regions and subcontractors?

Evidence

- Can the supplier show test results and production configuration evidence?

Commercial fit

Do costs, support and exit terms fit?

Provider oversight and audit evidence need a recurring cadence

Proposed cadence. Apply stricter sector, contract or agency requirements where relevant.

Ongoing management

Monthly during active migration

- Review milestones, blockers and changes.

- Quarterly for critical providers
- Refresh coverage, exceptions and evidence.

- At renewal or material change
- Reassess terms, dependencies and exit options.

Assurance and audit periods

Annual risk-based assurance review

- Reconcile the inventory and roadmap.

- Before and after each cutover
- Retain test results and configuration evidence.

- For each external report
- Check the review period, scope, exclusions and any gap since the period ended.

Practical Responses

Accountability stays with the organization

Proposed division of responsibilities

Keep internally

Own data priorities, risk acceptance, funding and critical-service decisions.

Use product providers

Obtain supported upgrades and product-specific migration instructions.

Use specialist support

Bring in discovery, cryptographic architecture or testing skills where capability is limited.

Validate together

Test the full service and recovery path. Retain independent evidence of acceptance.

Next Steps for In-House Counsel

1	**Map key suppliers and assess their terms**	Who holds your long-lived data or keys? Check the contracts
2	**Build a customer contracting playbook**	Standard PQC terms, flow-downs, and fallback positions
3	**Keep the board informed**	Put quantum risk on the oversight agenda, and document it
4	**Advise on updating the risk assessment**	Name quantum risk; record controls and any risk acceptance
5	**Support a transition plan**	Inventory, priorities, an owner, and dates tied to 2030–2035

Next Steps for CISOs, Technology & GRC

Unified approach for Cyber, AI, and Quantum (PQC) Readiness

Technology & Security

Unified CBOM & AI-BOM

Map cryptographic dependencies, long-lived data stores, AI models, and training data pipelines.

Dual Agility Architecture

Decouple architecture to seamlessly swap both PQC algorithms (FIPS 203/204/205) and AI models.

Pilot & Cutover Execution

Test hybrid key-exchange mechanisms and secure AI API transport connections in priority workloads.

Embedded Systems & Model Trust

Verify model weight signatures and zero-trust update paths for OT and edge devices.

Governance, Risk & Compliance

Joint Board Oversight

Integrate AI and Quantum (HNDL) risks into board agendas to satisfy Caremark duties and SEC Item 106.

Data Secrecy & HNDL Risk

Prioritize data with long secrecy lifecycles, especially proprietary information ingested by AI training pipelines.

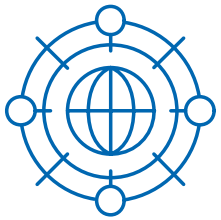
Third-Party Accountability

Update contracting playbooks to require unified PQC and AI vendor roadmaps, including FAR flow-downs.

Funded Delivery & Audit

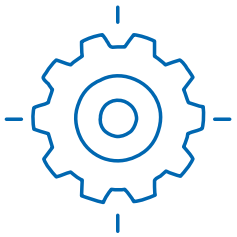
Assign executive owners, allocate budget for dual-readiness, and establish monthly/annual evidence logs.

Further reading and discussion



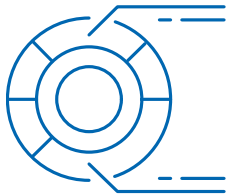
Technical foundations

NIST: Quantum Computing Explained and FIPS 203–205



Readiness and implementation

CISA, NSA and NIST: Quantum-Readiness



Policy and timelines

EO 14412 and OMB M-26-15 (2026)

NCSC: Timelines for migration to PQC

Thank You For Joining

Quantum computing creates opportunities and security obligations

Section 1: What quantum computing changes



A different computing model

Qubits use quantum states. Algorithms exploit interference and entanglement for particular problems.



Selective advantage

Quantum computers may outperform classical machines on some tasks. They will not accelerate every workload.



A capability still developing

Error correction and scale remain major engineering challenges. Timing of cryptographic disruption is uncertain.

What organizations can do with it

Scientific opportunity
Molecular and materials simulation could improve discovery. Benefits depend on useful, reliable hardware.



Business experimentation
Optimization and related applications warrant testing against the best classical alternatives.



Security preparation now
Post-quantum cryptography runs on conventional systems and supports migration before the threat arrives.



Sources: NIST, Quantum Computing Explained; NIST PQC standards (2024)

Where quantum threatens cryptography

Public-key mechanisms require the most urgent transition planning

Public-key cryptography

RSA and elliptic-curve mechanisms support key establishment and digital signatures.

- A sufficiently capable quantum computer running Shor's algorithm could defeat these mathematical protections.
- Consequences include disclosure of data and forged identities or signed software.

Symmetric cryptography

AES and hash functions face a different risk profile. Grover's algorithm offers a theoretical search speedup, with substantial practical costs.

- AES-256 remains an important part of defensive designs.
- Strong data encryption still depends on secure key exchange, key storage and implementation.

U.S. policy has moved from inventory toward migration execution

	Federal policy foundation	What clients should do with it
2022	NSM-10 and the Quantum Computing Cybersecurity Preparedness Act establish the federal transition foundation.	Determine whether federal systems, contracts or sector rules put your organization in scope.
2024–2025	NIST issued FIPS 203–205 in 2024. EO 14306 amended EO 14144 in June 2025.	Use approved standards and current requirements. Avoid relying on superseded summaries of the 2025 order.
2026	■ EO 14412 accelerates federal PQC migration. ■ OMB M-26-15 provides execution guidance for agencies. ■ National security systems follow a separate path.	■ Assess contract and procurement changes with counsel. ■ Translate obligations into system-level delivery dates. ■ Separate mandatory requirements from planning guidance.
IMPLICATION	Federal requirements shape supplier roadmaps and procurement expectations.	A federal deadline does not automatically apply to every private company.

Sources: Public Law 117-260; NIST FIPS 203–205; EO 14306; EO 14412; OMB M-26-15. Scope as of October 2026.

Applicability depends on the system, contract and jurisdiction

		EXPOSURE	WHAT TO VERIFY	PRACTICAL RESPONSE
CLIENT CONTEXT	Federal civilian systems	Direct agency requirements and implementation guidance	▪ System designation ▪ Agency scope ▪ Current OMB milestones	▪ Assign an accountable program owner and report against required milestones.
	Suppliers and contractors	Requirements may flow through contracts and procurements	▪ Contract clauses ▪ Customer security schedules ▪ Evidence obligations	▪ Agree deliverables, supported products and acceptance evidence with the customer.
	Other private organizations	Sector, privacy and contractual obligations remain relevant	▪ Jurisdiction and sector ▪ Data sensitivity ▪ Customer commitments	▪ Use a risk-based roadmap and document why the sequence fits business exposure.

Sources: EO 14412; OMB M-26-15; consultant recommendations. Obtain legal advice on applicability.

Critical services depend on encryption and digital trust

		CRYPTOGRAPHY	TYPICAL PROVIDERS	CLIENT ACCOUNTABILITY
SERVICE CHAIN	Customer access and transactions	Transport security Identity and certificates Transaction signatures	▪ Cloud, SaaS and identity providers ▪ Payment and connectivity partners	▪ Map every connection and authentication dependency for the service.
	Sensitive data and recovery	Data encryption Key wrapping and storage Recovery credentials	▪ Cloud storage and backup providers ▪ Key management and HSM vendors	▪ Confirm the key lifecycle, protection period and ability to restore data.
	Software and device trust	Code signing Firmware verification Device identity	▪ Software publishers ▪ Equipment manufacturers ▪ Managed service providers	▪ Confirm the update path, verification chain and replacement plan.

Illustrative cross-industry examples and consultant recommendations, informed by CISA/NSA/NIST.

Policy milestones guide planning, but client exposure sets the pace

U.S. FEDERAL MILESTONES



2026–2027
Agency planning and discovery under OMB M-26-15.



2030
PQC key establishment for covered high-value and high-impact federal systems.



2031
PQC digital signatures for those covered federal systems.

Agency plans: within 120 days of June 24, 2026, under M-26-15

CLIENT ROADMAP AND INTERNATIONAL BENCHMARK



1 **Next 90 days**
Assign ownership, inventory priority services and engage suppliers.



2 **Next 6–12 months**
Test a prioritized use case and fund dependency remediation.



3 **UK guidance**
2028 discovery and planning. 2031 priority migration. 2035 completion.



4 **Broader U.S. path**
M-26-15 sets phased migration toward 2035 for federal agencies.

Federal dates have defined scope. UK dates are guidance. Client planning horizons are proposed.

Sources: EO 14412; OMB M-26-15; NCSC PQC migration timelines. Policy reference: October 2026.