ETSI/IQC Quantum Safe Cryptography Conference 2026

The New US Cybersecurity Strategy: National Mandates, Industry Response & the Road to Quantum Resilience

Presented by:

QuSecure

17/06/2026

QuSecure

US Industry & Government Collaboration on

The New Cybersecurity Strategy: National Mandates, Industry Response & the Road to Quantum Resilience

NIST PQC Standards | Executive Orders | NSM-10 | CNSA 2.0 | Industry Migration

THE QUANTUM THREAT LANDSCAPE

WHY PQC IS AN URGENT NATIONAL PRIORITY

The Timeline

Expert consensus: cryptographically relevant quantum computers by ~2030 ± 2 years. IBM, Google & IonQ roadmaps converge on late 2020s.

$7.1B

Estimated US federal PQC migration cost (2025–2035)

2030

Consensus estimate for Q-Day arrival

Harvest Now, Decrypt Later

Nation-state adversaries are capturing encrypted traffic today to decrypt retroactively once quantum capability matures — a clear and present danger.

46.2%

CAGR growth of global PQC market through 2030

2027

NSA CNSA 2.0 deadline for new National Security Systems

Symmetric algorithms (AES-256) remain quantum-safe. The urgent gap is in public-key / asymmetric cryptography used for authentication, key exchange, and digital signatures.

THE QUANTUM THREAT LANDSCAPE

WHY PQC IS AN URGENT NATIONAL PRIORITY

RSA & ECC Vulnerable

Shor's algorithm breaks RSA, ECDSA, ECDH and all widely deployed asymmetric cryptography. ***2026 research reduced qubit requirements to ~10K to 100K physical qubits.***

$7.1B

Estimated US federal PQC migration cost (2025–2035)

2030

Consensus estimate for Q-Day arrival

Market Growth Context

Compound Annual Growth Rate (CAGR) through the early 2030s. This growth is heavily driven by increasing vulnerabilities of legacy encryption to future quantum computing attacks. ***The BFSI (Banking, Financial Services, and Insurance),*** defense, and cloud service sectors lead adoption.

46.2%

CAGR growth of global PQC market through 2030

2027

NSA CNSA 2.0 deadline for new National Security Systems

US GOVERNMENT PQC POLICY FRAMEWORK

A DECADE OF REGULATORY MOMENTUM — KEY MANDATES & MILESTONES

2022

NSM-10 & CISA Initiative

National Security Memorandum-10 directs full PQC migration by 2035; CISA launches PQC Initiative with industry partners

2023

OMB M-23-02

Mandates annual agency cryptographic inventories; CISA, NSA & NIST publish joint migration guidance for critical infrastructure

Aug 2024

NIST PQC Standards Released

FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) & FIPS 205 (SLH-DSA) finalized — first formal quantum-resistant standards worldwide

Jun 2025

Executive Order 14306

EO directing CISA/NSA to publish PQC product categories list by Dec 1, 2025; TLS 1.3 mandated by Jan 2030

Jan 2027

CNSA 2.0 Deadline

All new National Security Systems must be quantum-resistant per NSA's Commercial National Security Algorithm Suite 2.0

2035

NSM-10 Full Migration Goal

All prioritized federal systems to achieve PQC compliance; estimated $7.1B government-wide investment

INDUSTRY'S COLLECTIVE VIEW ON PQC

CONSENSUS POSITIONS ACROSS US SECTORS

BROAD CONSENSUS

- PQC migration is non-negotiable
- **Crypto-agility must be built into all new systems from design stage**
- Hybrid classical+PQC deployments are the immediate practical path forward
- NIST FIPS 203/204/205
- Third-party cryptographic inventories are an immediate priority

KEY CONCERNS

- Migration complexity**: legacy systems have long replacement cycles**
- Supply chain risk — PQC must extend to vendors & third parties
- **Skills gap/Awareness:** workforce does not yet have sufficient PQC expertise
- **Performance overhead of PQC algorithms on constrained devices**
- International standards fragmentation could hurt B2B communications

INDUSTRY ASKS OF GOV

- Clearer procurement guidelines & PQC product certification paths
- **Funding incentives for SMBs to begin PQC transitions**
- Reasonable compliance timelines with phased enforcement
- ***Shared threat intelligence on HNDL attack campaigns***
- Government-led pilot programs to reduce transition risk

INDUSTRY–GOVERNMENT PARTNERSHIP MECHANISMS

FORMAL COLLABORATION CHANNELS DRIVING PQC TRANSITION

NCCoE PQC Migration Consortium

NIST's National Cybersecurity Center of Excellence leads **a 40+ member consortium** including AWS, Cisco, Microsoft, IBM, JPMorgan Chase, Dell, Thales & DigiCert. Consortium has produced NIST SP 1800-38 testing artifacts and integration frameworks covering cryptographic discovery, interoperability & performance.

IETF & International Standards

US industry leads standards working groups to integrate NIST PQC algorithms into TLS, SSH, S/MIME, and other protocols. Google, Cloudflare, and Palo Alto Networks are actively deploying PQC in production TLS traffic. Coordination ensures US & global standards converge.

NSA CNSA 2.0 Vendor Engagement

NSA works directly with defense contractors and national security vendors to enforce **CNSA 2.0 timelines. By Jan 2027, all new NSS products must support quantum-resistant algorithms.** Vendors aligning hardware (HSMs, network encryptors) with FIPS 203/204/205 standards.

SECTOR-BY-SECTOR INDUSTRY ACTION

HOW KEY US INDUSTRIES ARE IMPLEMENTING PQC IN PRACTICE

Industry	Companies	Implementation Details	Status
Big Tech & Cloud	Google, Microsoft, Amazon, Apple, Cloudflare	Google integrating ML-KEM in Chrome TLS. Microsoft adding PQC to Windows 11 & Azure. Apple deployed PQ3 in iMessage (HNDL defense). Cloudflare running PQC in production TLS. AWS building PQC into KMS.	LEADING
Financial Services	JPMorgan Chase, Citi, SWIFT, Federal Reserve	JPMorgan Chase in NCCoE consortium; piloting PQC for inter-bank payment systems. Federal Reserve published HNDL blockchain analysis. SWIFT coordinating member bank PQC readiness.	PROGRESSING
Defense & Aerospace	Lockheed, Raytheon, Northrop, L3Harris	NSA CNSA 2.0 mandates direct vendor engagement. Defense contractors updating HSMs, satellite comm, and weapons system authentication. DoD separately developing classified migration cost estimates for NSS.	MANDATED
Telecom & Networking	Cisco, Palo Alto Networks, Verizon, AT&T	Cisco integrating PQC into IOS-XE and network encryptors. Palo Alto deploying PQC-capable next-gen firewalls. Carriers updating 5G/6G protocol stacks to support hybrid PQC modes.	ACTIVE
Healthcare & Critical Infrastructure	HHS partners, Energy sector, ICS vendors	HHS issuing PQC guidance for medical device manufacturers. Energy sector OT/ICS vendors engaging DHS CISA for long-lifecycle system migration. GSA providing compliant acquisition pathways for federal health agencies.	EARLY STAGE

EXECUTIVE ORDER 14306: THE NEW MANDATE

JUNE 2025 EO — WHAT INDUSTRY MUST KNOW

KEY PROVISIONS OF EO 14306

- CISA & NSA directed to publish list of PQC-ready product categories by Dec 1, 2025 — updated regularly
- Federal agencies must support TLS 1.3 or later by January 2, 2030, with full PQC implementation
- National Security Systems explicitly included — expanding scope beyond civilian agencies
- Vendors supplying federal agencies must align products with CISA's PQC product categories list for procurement eligibility
- Builds on and reaffirms NSM-10 (Biden, 2022) as foundational framework — bipartisan continuity on PQC
- EO 14306 adds amendments to EO 14144, showing quantum cybersecurity is a sustained national priority across administrations

INDUSTRY IMPACT

Procurement Gate:
PQC capability now a federal procurement requirement — non-compliant vendors excluded from federal market

Product Roadmaps:
Hardware & software vendors must accelerate PQC integration into HSMs, firewalls, OS, and cloud services

Compliance Timeline:
Dec 2025 CISA list → Dec 2025 assessment → 2027 NSS deadline → Jan 2030 TLS 1.3 mandate

Bipartisan Signal:
Consistent PQC priority across Biden & Trump administrations signals long-term regulatory certainty for industry investment

MIGRATION CHALLENGES & INDUSTRY SOLUTIONS

THE PATH TO CRYPTO-AGILITY: BARRIERS AND HOW INDUSTRY IS OVERCOMING THEM

CHALLENGE	INDUSTRY RESPONSE
Cryptographic Discovery**: Organizations don't know where all cryptographic assets reside in complex systems**	Commercial ACDI tools now automate continuous cryptographic inventory — no more manual one-time audits
Legacy System Lifespan: **Industrial, medical, and defense systems have 15-30 year lifecycles incompatible with rapid migration**	Hybrid/layered approaches**: wrap legacy systems with PQC-capable gateways**; use network-level encryptors as interim shield
Performance Overhead: PQC algorithms (esp. signatures) have larger key sizes and higher compute demands on constrained devices	Silicon-level integration: embedding PQC acceleration into chipsets; HSM vendors adding hardware co-processors
Skills Gap: Most enterprise security teams lack PQC implementation expertise; cryptographers are scarce	NIST SP 1800-38 practice guides, NCCoE playbooks, and vendor training programs lower the barrier
Supply Chain Complexity: PQC must cascade through entire vendor ecosystem — impossible to secure only the prime contractor	Industry consortia (e.g., Post-Quantum Cryptography Alliance / Linux Foundation) developing interoperability standards and shared testing suites

PQC ADOPTION READINESS BY SECTOR

CURRENT MIGRATION PROGRESS ACROSS US INDUSTRY VERTICALS (2026 ASSESSMENT)

SCORING METHODOLOGY

Cryptographic Inventory Complete — **30%**

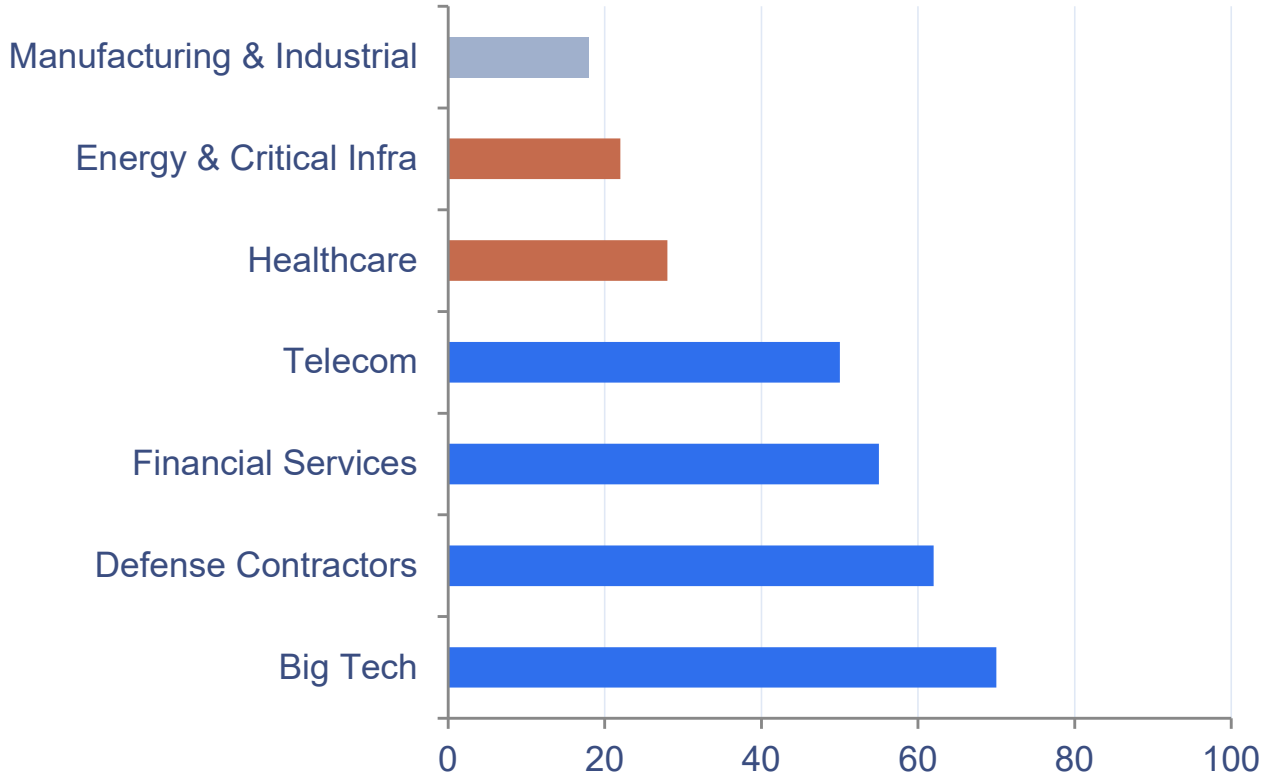
PQC Pilot Deployments Underway — **25%**

Staff Training & Upskilling — **20%**

Vendor/Supply Chain Engagement — **15%**

Policy & Budget Allocation — **10%**

Note: Scores are composite estimates based on NCCoE consortium reports, CISA agency assessments, and industry analyst data (2026). Score of 100 = full PQC migration complete.



STRATEGIC RECOMMENDATIONS

FOR ORGANIZATIONS NAVIGATING THE US PQC LANDSCAPE

01 **Immediate**

Launch Cryptographic Inventory NOW

Deploy ACDI tooling to identify all RSA, ECDH, ECDSA, and Diffie-Hellman usage across your enterprise, cloud, and supply chain. OMB M-23-02 compliance requires it; CISA provides free tooling guidance.

02 **0–6 Months**

Develop a Quantum Readiness Roadmap

Map cryptographic assets against risk priority. Build phased migration plan following NIST SP 1800-38 framework. Apply Mosca's Theorem to identify data with long confidentiality requirements.

03 **6–18 Months**

Pilot Hybrid PQC Deployments

Begin hybrid TLS (classical + ML-KEM) in low-risk environments. Engage NCCoE consortium resources. Test FIPS 203/204/205 algorithm performance in your specific hardware & software environment.

04 **Ongoing**

Align Procurement with CISA PQC List

Ensure new hardware, software & services purchases support CISA's PQC product categories. For federal vendors: non-compliance risks exclusion from federal marketplace under EO 14306.

05 **Strategic**

Invest in Workforce & Supply Chain

Upskill security and engineering teams via NIST, ISACA, and vendor PQC training. Extend PQC requirements contractually to your supply chain. Engage industry consortia for shared tooling.

06 **Ongoing**

Engage Government Channels

Participate in NCCoE working groups. Monitor NSA CNSA 2.0 compliance deadlines actively. Leverage GSA acquisition pathways for compliant PQC product procurement.

QuSecure

THE WINDOW IS OPEN.
THE CLOCK IS RUNNING.

The US government has established clear mandates, standards, and timelines. Industry has engaged — but migration at scale is still in early stages across most sectors. The bipartisan regulatory consensus, NSA enforcement deadlines, and Harvest-Now-Decrypt-Later threat demand immediate, sustained action.

ASSESS	PLAN	ACT
Complete cryptographic inventory	Build quantum readiness roadmap	Begin hybrid PQC deployments

Key Resources: NIST PQC (csrc.nist.gov/pqc) · CISA PQC Initiative (cisa.gov/quantum) · NCCoE SP 1800-38 · NSA CNSA 2.0