

INTELLIGENCE BRIEF

Federal Post-quantum Deadlines Are Set While Attack Estimates Keep Falling

A June 2026 executive order and OMB memo set 2030 and 2031 federal dates, and Google moved its own migration to 2029. Inventory your cryptography, turn on hybrid key exchange, and put PQC into every purchase.

EDITION

Fall/Winter 2026/2027 Edition

TR-01 · Technology risk

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ONGOING RISK

OMB says a cryptographically relevant quantum computer is not yet known to exist, but federal migration dates now run from 2030, and data collected today for later decryption is an acknowledged policy concern. [1]

HEADLINE NUMBERS

Dec 31, 2030

federal deadline for PQC key establishment on high-value and high-impact systems [3]

70%

browser traffic to Cloudflare using hybrid ML-KEM, September 2026 [5]

<500,000

physical qubits in Google's ECDLP-256 attack estimate [4]

28% to 49%

expert odds of a cryptographically relevant quantum computer within 10 years [10]

KEY FACTS

STANDARDS

FIPS 203, 204 and 205 final since August 13, 2024; FIPS 206 (FN-DSA) not yet on NIST's FIPS list [2]

FEDERAL DATES

High-value and high-impact systems: PQC key establishment by Dec 31, 2030, digital signatures by Dec 31, 2031 [3]

AGENCY PLANS

Civilian agency migration plans due to OMB 120 days after June 24, 2026, about October 22; full migration by 2035 [1]

ATTACK ESTIMATES

Google: elliptic curve (ECDLP-256) attack with fewer than 500,000 physical qubits [4]

ADOPTION

About 70% of browser traffic to Cloudflare uses hybrid ML-KEM; about 15% of origins do [5]

VENDOR TIMELINES

Google set a 2029 migration timeline and urged other engineering teams to follow [6]

02 What Happened

The original edition, written in February 2026, argued that the window for migration was closing as new factoring estimates and nation-state data collection raised the urgency. Since then the United States has put dates on it: an executive order signed June 22, 2026 and an OMB memo two days later require federal high-value assets and high-impact systems to use post-quantum key establishment by December 31, 2030 and post-quantum digital signatures by December 31, 2031. Google and Cloudflare both set 2029 targets, and published attack estimates fell again in March 2026.

- NIST's three final standards, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA), remain the only final post-quantum FIPS; FIPS 206 (FN-DSA) does not yet appear on NIST's FIPS list.
- OMB M-26-15 gives civilian agencies 120 days from June 24, 2026 to submit migration plans and lays out five phases through 2035; it does not cover national security systems.
- EO 14412 tells the FAR Council to propose a rule within 180 days requiring covered contractors to comply by December 31, 2030 with NIST FIPS, including those that incorporate post-quantum algorithms.
- Hybrid post-quantum key exchange now protects about 70 percent of browser traffic reaching Cloudflare, but post-quantum authentication lags: Cloudflare expects the first ML-DSA certificates in the web PKI in early 2027.
- The Global Risk Institute's March 2026 survey of 26 experts put the odds of a cryptographically relevant quantum computer at 28 to 49 percent within 10 years and 51 to 70 percent within 15.
- The proposed HIPAA Security Rule overhaul, which discusses quantum computing, is now projected for a final rule in July 2027 rather than the May 2026 the original expected.

03 How It Works

01 Collect encrypted data now

EO 14412 describes adversaries collecting U.S. information now and decrypting it later once large-scale quantum computers are operational. Recorded sessions that used classical key exchange are the raw material.

02 Keep what stays valuable

OMB tells agencies to prioritize systems that hold data expected to remain mission-sensitive in 2030. Identity, health, student and government records keep their value for years after capture.

03 Wait for a capable quantum computer

OMB says a cryptographically relevant quantum computer is not yet known to exist but may arrive in the coming decade. Estimates of the qubits required have fallen repeatedly, most recently in March 2026.

04 Break the key exchange

OMB lists RSA, Diffie-Hellman and elliptic curve methods as quantum-vulnerable. Hybrid ML-KEM, now common in browsers, protects new sessions against later decryption.

05 Forge identity later

Signatures cannot be harvested and cracked retroactively, but they must move before a capable computer exists. Google reprioritized authentication services, and Cloudflare notes the certificate chain is the slow part.

04 Who Is at Risk

Any organization whose data must stay confidential for a decade or more, and any organization that sells to or supports federal agencies. Exposure follows how long the data stays valuable and how many vendors sit in the chain.

- Federal agencies and contractors: EO 14412 and M-26-15 set dates, and a FAR rule is due for contractors.
- State, local and education agencies holding long-retention records such as identity, health and student data; no state mandate was confirmed in this review.
- Healthcare organizations: the HIPAA Security Rule proposal discusses quantum computing, with a final rule now projected for July 2027.
- Financial institutions: the G7 Cyber Expert Group roadmap targets critical systems in the 2030 to 2032 window and the rest around 2035.
- Critical infrastructure and operational technology: EO 14412 tells sector risk management agencies to help operators plan, and CISA's product list excludes OT and IoT devices.

Sectors in scope: federal agencies and contractors, state, local government and education, healthcare, financial services, critical infrastructure and operational technology.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 Executive Order 14412 (June 22, 2026) sets the first hard federal post-quantum dates: high-value assets and high-impact systems use PQC for key establishment by December 31, 2030 and for digital signatures by December 31, 2031. It also directs a FAR proposed rule for contractors within 180 days, NIST work to speed cryptographic module validation within 180 days, and CISA guidance on a cryptographic bill of materials within 270 days.

SOURCE 3

02 OMB M-26-15 (June 24, 2026) turns the order into agency tasks: a migration plan to OMB and the National Cyber Director within 120 days, a five-phase schedule (planning 2026 to 2027, pilots 2027 to 2028, prioritized migration 2028 to 2030, signatures 2031, full migration 2035), TLS 1.3 by January 2, 2030, automated cryptographic inventory feeding a cryptographic bill of materials, and alignment with NIST IR 8547.

SOURCE 1

03 Google set a 2029 target for its own post-quantum migration on March 25, 2026, said encryption is urgent now because of store-now-decrypt-later attacks, moved authentication services up its priority list, and recommended that other engineering teams follow suit.

SOURCE 6

04 Published attack estimates fell again. Google Quantum AI said on March 31, 2026 that ECDLP-256 can be attacked with fewer than 1,200 logical qubits and under 500,000 physical qubits in minutes, about a 20-fold reduction, and published a zero-knowledge proof so others can verify the claim without the attack details.

SOURCE 4

05 NIST's additional signature on-ramp reached Round 3 on May 14, 2026, while no FIPS 206 (FN-DSA) or HQC draft appeared on NIST's FIPS list as of October 13, 2026.

SOURCE 7

06 Hybrid post-quantum key exchange is now the norm: Cloudflare's September 29, 2026 figures show about 70 percent of browser traffic to its network and about 15 percent of origins using hybrid ML-KEM.

SOURCE 5

07 The HIPAA Security Rule overhaul proposed in January 2025, whose preamble discusses quantum computing, now shows a projected final rule date of July 2027 on the regulatory agenda, listed as a long-term action.

SOURCE 8

08 Cloudflare moved its full post-quantum target, including authentication, to 2029 on April 7, 2026, citing new research and Google's accelerated timeline, with milestones of mid-2026 for post-quantum authentication to origins, mid-2027 for visitor connections using Merkle Tree Certificates and early 2028 for its SASE suite.

SOURCE 9

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Build a cryptographic inventory now, using automated discovery for certificates, TLS endpoints, VPNs, code signing and embedded keys.**

OMB's memo calls the inventory the foundation of every migration plan and expects automation and a cryptographic bill of materials.

02 **Prioritize systems by how long their data stays sensitive, starting with identity, health, student and government records, and by exposure to the internet.**

Data captured today can be decrypted later, so long-lived data is the first thing to protect.

03 **Turn on hybrid ML-KEM key exchange wherever your stack already supports it, and move TLS endpoints to TLS 1.3.**

Browsers, Apple platforms and major CDNs already negotiate it, and hybrid key exchange is the standard route to protection against later decryption.

04 **Write post-quantum support and cryptographic agility into every software, network and cloud purchase, using CISA's product categories list as the reference.**

The FAR rule due under EO 14412 will carry federal requirements to contractors and the vendors behind them.

05 **Plan the signature and certificate migration as its own track: PKI, code signing, device identity and ML-DSA readiness.**

Authentication has the longest dependency chain, and Cloudflare expects the first ML-DSA certificates in the web PKI only in early 2027.

06 **Use only NIST-standardized algorithms, and treat quantum key distribution and pre-shared-key products sold as quantum-safe with caution.**

The Defense Department's November 2025 memo bars quantum key distribution for security functions without an exception and sets a 2030 phase-out of pre-shared-key approaches.

07 **Map your regulatory clock: federal contractor requirements, the January 1, 2027 CNSA 2.0 acquisition date for national security systems, HIPAA, and financial sector roadmaps.**

Dates now differ by sector, from 2030 for federal key establishment to 2035 for full migration.

08 **Ask a qualified partner to run a cryptographic discovery and migration roadmap if you lack the staff.**

Z7 Solutions™ offers cryptographic inventory and PQC migration roadmap engagements for federal, SLED, healthcare and financial organizations.

07 Sources

[1] **OMB Memorandum M-26-15, Execution of the Migration to Post-Quantum Cryptography** Executive Office of the President, Office of Management and Budget · June 24, 2026. https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

[2] **FIPS publications list** NIST Computer Security Resource Center · Checked October 13, 2026. https://csrc.nist.gov/publications/fips

[3] **Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks (91 FR 38483)** The White House, published in the Federal Register · Signed June 22, 2026; Federal Register June 25, 2026. https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

[4] **Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly** Google Research (Ryan Babbush and Hartmut Neven, Google Quantum AI) · March 31, 2026. https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/

[5] **Is your domain using post-quantum encryption? Now you can see for yourself** Cloudflare · September 29, 2026. https://blog.cloudflare.com/post-quantum-visibility/

[6] **We're setting a timeline for post-quantum cryptography migration to 2029** Google (Heather Adkins and Sophie Schmieg) · March 25, 2026. https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

[7] **Additional Digital Signature Schemes for the NIST PQC Standardization Process** NIST Computer Security Resource Center · Round 3 candidates announced May 14, 2026. https://csrc.nist.gov/projects/pqc-dig-sig

[8] **Unified Agenda entry, HIPAA Security Rule to Strengthen the Cybersecurity of ePHI (RIN 0945-AA22)** reginfo.gov (Office of Information and Regulatory Affairs) · Agenda edition pubId 202510; accessed October 13, 2026. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22

[9] **Cloudflare targets 2029 for full post-quantum security** Cloudflare · April 7, 2026. https://blog.cloudflare.com/post-quantum-roadmap/

[10] **Quantum Threat Timeline Report 2025** Global Risk Institute and evolutionQ (Mosca and Piani) · March 9, 2026. https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

[11] **The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes (arXiv:2602.11457)** Iceberg Quantum authors, via arXiv · Submitted February 12, 2026; revised May 5, 2026. https://arxiv.org/abs/2602.11457

[12] **How to factor 2048 bit RSA integers with less than a million noisy qubits (arXiv:2505.15917)** Craig Gidney, via arXiv · Submitted May 21, 2025. https://arxiv.org/abs/2505.15917

[13] **Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits (arXiv:2603.28627)** Cain, Xu, King, Picard, Levine, Endres, Preskill, Huang and Bluvstein, via arXiv · Submitted March 30, 2026. https://arxiv.org/abs/2603.28627

[14] **IBM Quantum roadmap** IBM · Accessed October 13, 2026. https://www.ibm.com/roadmaps/quantum/

[15] **The IPO Buzz: Quantinuum priced upsized IPO at $60, $5 above range** IPO Scoop · June 2026. https://www.iposcoop.com/the-ipo-buzz-quantinuum-priced-upsized-ipo-at-60-5-above-range/

[16] **Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System (AA25-239A)** CISA, NSA, FBI and partners · August 27, 2025; revised September 3, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[17] **FCC rolls back cybersecurity rules for telcos despite state hacking risks** BleepingComputer · November 21, 2025. https://www.bleepingcomputer.com/news/security/fcc-rolls-back-cybersecurity-rules-for-telcos-despite-state-hacking-risks/

[18] **Quantum Threat: The Trillion-Dollar Security Race Is On (Citi Institute), as summarized by PostQuantum.com** PostQuantum.com · January 18, 2026. https://postquantum.com/security-pqc/citi-quantum-threat-report/

[19] **State of the post-quantum Internet in 2025** Cloudflare · October 2025. https://blog.cloudflare.com/pq-2025/

[20] **Prepare for quantum-secure cryptography in TLS (iOS 26, iPadOS 26, macOS Tahoe 26)** Apple Support · Accessed October 13, 2026. https://support.apple.com/en-us/122756

[21] **Signal Protocol and Post-Quantum Ratchets (SPQR)** Signal · October 2, 2025. https://signal.org/blog/spqr/

[22] **Quantum-safe security: Progress towards next-generation cryptography** Microsoft Security Blog · August 20, 2025. https://www.microsoft.com/en-us/security/blog/2025/08/20/quantum-safe-security-progress-towards-next-generation-cryptography/

[23] **Why we cannot wait for better post-quantum signature algorithms** Cloudflare · July 9, 2026. https://blog.cloudflare.com/ml-dsa-will-have-to-do/

[24] **NIST selects HQC as fifth algorithm for post-quantum encryption** NIST Computer Security Resource Center · March 11, 2025. https://csrc.nist.gov/news/2025/hqc-announced-as-a-4th-round-selection

[25] **Product Categories for Technologies That Use Post-Quantum Cryptography Standards** CISA · January 23, 2026. https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards

[26] **Pentagon CIO orders rapid shift to post-quantum crypto** MeriTalk · December 11, 2025 (reporting a memo dated November 18, 2025). https://meritalk.com/articles/pentagon-cio-orders-rapid-shift-to-post-quantum-crypto/

[27] **Executive Order 14306, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity (90 FR 24723)** The White House, published in the Federal Register · Signed June 6, 2025; Federal Register June 11, 2025. https://www.govinfo.gov/content/pkg/FR-2025-06-11/pdf/2025-10804.pdf

[28] **Senate Commerce Committee unanimously passes National Quantum Initiative Reauthorization Act** Quantum Computing Report · April 19, 2026. https://quantumcomputingreport.com/senate-commerce-committee-unanimously-passes-national-quantum-initiative-reauthorization-act/

[29] **U.S. Quantum Policy Bill Advances to Full House Consideration** The Quantum Insider · May 1, 2026. https://thequantuminsider.com/2026/05/01/u-s-quantum-policy-bill-advances-to-full-house-consideration/

[30] **CNSA 2.0 deep dive** PostQuantum.com · Accessed October 13, 2026. https://postquantum.com/post-quantum/cnsa-2-0/

[31] **EU reinforces its cybersecurity with a coordinated post-quantum cryptography roadmap** European Commission · June 23, 2025. https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography

[32] **Timelines for migration to post-quantum cryptography** UK NCSC · March 20, 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[33] **Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)** Government of Canada, CCCS · June 2025. https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

[34] **The G7 Cyber Expert Group publishes the roadmap for the transition of the financial sector to post-quantum cryptography** Banca d'Italia · January 13, 2026. https://www.bancaditalia.it/media/notizia/the-g7-cyber-expert-group-publishes-the-roadmap-for-the-transition-of-the-financial-sector-to-post-quantum-cryptography/

[35] **HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information (90 FR 898)** HHS, published in the Federal Register · January 6, 2025. https://www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf

[36] **FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard** NIST Computer Security Resource Center · August 13, 2024; planning note November 17, 2025. https://csrc.nist.gov/pubs/fips/203/final

NEXT STEP

What does this mean for your security?

Bring your questions about Post-quantum cryptography readiness, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/
- Qilin still hits hospitals and infrastructure
  More from the edition · z7solutions.com/z7-cyber/qilin-part-2/
- LockBit 5.0 returns after Operation Cronos
  More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL	844-974-8669
EMAIL	sales@z7solutions.com
BOOK A SECURITY CONVERSATION	Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.