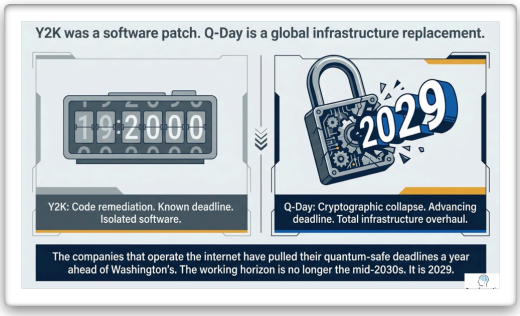
Transformativ IP

Q-Day Keeps Moving Up

Microsoft, Google and Cloudflare Now Say 2029.

The three companies that operate much of the internet have pulled their quantum-safe deadlines a year ahead of Washington's. The estimated cost of breaking RSA fell 20-fold in eighteen months. And the field's most prominent skeptic just changed his mind.



For a decade the answer to when a quantum computer would break the encryption underpinning global commerce was comfortably distant: the mid-2030s. That estimate has been revised three times in eighteen months, always in the same direction. In May 2025 a Google researcher cut the hardware needed to factor a 2,048-bit RSA key from 20 million qubits to fewer than one million — a 20-fold reduction, under the same physical assumptions as his own earlier figure.

In March 2026 Google set an internal deadline of 2029; Cloudflare matched it thirteen days later. In June the White House made 2030 and 2031 binding for federal systems and their contractors, France began stripping certification from products without quantum-resistant encryption, and Microsoft's Azure CTO wrote that cryptographically relevant quantum computers *could arrive sooner than previously expected*. What they say, in unison, is that they can no longer rule it out — and that the migration TO PQC takes longer than the time now left for healthcare and finance using traditional PQC solutions.

Transformativ IP offers PQC Migration in under 90 days with no rip-and-replace and 100% software.

THE SALIENT FACTS

- **RSA got 20x cheaper to break in eighteen months.** Google's Craig Gidney cut the estimate from 20 million qubits (2019) to **under one million** (2025) — same hardware assumptions. arXiv:2505.15917 *→ The Math*
- **Elliptic curve falls first, and in minutes.** Google Quantum AI with Stanford and the Ethereum Foundation: **under 500,000 physical qubits**. The authors withheld their own attack circuits, publishing a zero-knowledge proof instead. Whitepaper *→ The Math*
- **Three infrastructure giants, one date, reached independently.** Google (Mar. 25), Cloudflare (13 days later), Microsoft (Jun. 30) — all **2029**. *→ The Companies*
- **Microsoft's Azure CTO, on the record:** "cryptographically relevant quantum computers could arrive sooner than previously expected." Microsoft Security Blog
- **The field's leading skeptic reversed himself.** Scott Aaronson, after two decades deflating quantum hype: trusted hardware experts now say such a machine "ought to be possible by around 2029." *→ The Skeptic*
- **It is law now, not guidance.** Executive Order 14412 (Jun. 22, 2026): federal encryption by **Dec. 31, 2030**, authentication by **2031** — contractors bound via the acquisition regulation. Federal Register
- **France attached a penalty.** From **2027**, ANSSI stops certifying products without quantum-resistant encryption. No certificate, no contract. *→ Washington & Paris*

- **The old number was 2035.** NIST disallows RSA and ECC after 2035. The vendors are now a year ahead of Washington, six ahead of NIST. *→ How the Date Moved*
- **It is underway without you.** Over **65%** of human traffic to Cloudflare is already post-quantum encrypted — free on every plan since 2022. Cloudflare
- **For long-lived data the deadline has passed.** Harvest now, decrypt later: EO 14412 warns adversaries may already be collecting. *→ Why the Date May Not Matter*
- **Two cryptographic transitions collide in 2029.** The CA/Browser Forum's 47-day certificate lifespan takes full effect the same year. *→ What Boards Are Told*

How the Date Moved

The revision has been steady, public, and one-directional. Each entry below is a dated primary source, not a forecast.

Date	Development	Implied Horizon
2019	Gidney & Ekerå estimate RSA-2048 falls in 8 hours to a 20-million-qubit machine. Widely read as decades away.	2040s
2022	NSA issues CNSA 2.0 for national security systems.	2030–2033
2024–25	NIST IR 8547 deprecates quantum-vulnerable algorithms after 2030, disallows after 2035.	2035
May 2025	Gidney cuts the RSA-2048 estimate to fewer than 1 million noisy qubits, under a week.	Compressed 20x
Nov 2025	Aaronson calls a fault-tolerant machine running Shor's algorithm "a live possibility" before the next U.S. presidential election.	2028
Mar 25, 2026	Google sets a company-wide 2029 PQC migration timeline.	2029
Mar 30, 2026	Google/Stanford/Ethereum Foundation: ECC-256 falls to under 500,000 physical qubits.	Compressed again
Apr 7, 2026	Cloudflare matches 2029, including authentication.	2029
Apr 2026	Aaronson: trusted hardware experts say a CRQC "ought to be possible by around 2029."	2029
Jun 16, 2026	France's ANSSI to halt certification of non-quantum-safe products from 2027.	2027 (procurement)
Jun 22, 2026	EO 14412 makes 2030/2031 binding for federal systems and contractors.	2030–2031
Jun 30, 2026	Microsoft accelerates its Quantum Safe Program to 2029.	2029

The pattern is the story. In eighteen months the working horizon compressed from the mid-2030s to the end of this decade, and not one revision moved in the other direction.

The Math That Moved It

The deadlines did not move because a quantum computer appeared. They moved because the estimated price of the attack collapsed — twice.

RSA: from 20 million qubits to fewer than one million

In 2019, Craig Gidney of Google and Martin Ekerå of KTH published what became the industry's reference figure: a 2,048-bit RSA integer could be factored in eight hours by a machine with **20 million noisy qubits** (arXiv:1905.09749). In May 2025, Gidney revised his own number. The same integer, he estimated, could be factored in **under a week with fewer than one million noisy qubits** (arXiv:2505.15917).

What makes the revision credible to cryptographers is what did not change. Both papers assume the same square qubit grid with nearest-neighbour connections, the same 0.1% gate error rate, the same one-microsecond surface code cycle and ten-microsecond control reaction time. The 20-fold reduction came from algorithmic work — approximate residue arithmetic, yoked surface codes, magic state cultivation — not from relaxing the hardware assumptions. Google's own security blog described it as a **20-fold decrease** (Tracking the Cost of Quantum Factoring).

The same blog post supplies the counterweight, and executives should hold both numbers at once: quantum computers at relevant error rates today have **on the order of 100 to 1,000 qubits**.

Elliptic curve: under 500,000 physical qubits, and minutes to run

On March 30, 2026 — five days after Google announced its 2029 deadline — nine researchers from Google Quantum AI, UC Berkeley, Stanford and the Ethereum Foundation published resource estimates for the 256-bit elliptic curve discrete logarithm problem on secp256k1, the curve behind most digital signatures and every major cryptocurrency. The authors include Craig Gidney, Ryan Babbush, Hartmut Neven, Stanford cryptographer Dan Boneh and the Ethereum Foundation's Justin Drake (whitepaper PDF, arXiv:2603.28846).

- Shor's algorithm runs with either **≤1,200 logical qubits and ≤90 million Toffoli gates**, or ≤1,450 logical qubits and ≤70 million gates.
- On standard superconducting assumptions: **fewer than 500,000 physical qubits**, with runtime in minutes — roughly a 20-fold reduction from the prior best estimate of about 9 million.
- ECC needs roughly 100 times fewer gates than RSA-2048 — 70 to 90 million versus about 6.5 billion. **Elliptic curve cryptography breaks before RSA does.**

One detail deserves a board's attention more than the qubit count. The authors declined to publish their own circuits, using a **zero-knowledge proof** to demonstrate the results hold without disclosing how. Researchers treated their own findings as an operational hazard.

A separate paper released the same week, from Caltech and UC Berkeley researchers behind the startup Oratomic, put Shor's algorithm against ECC-256 within reach of roughly **10,000 reconfigurable atomic qubits**. Cloudflare cited both papers as the trigger for pulling its deadline forward.

What the Companies Actually Committed To

Google — March 25, 2026

Heather Adkins, vice president of security engineering, and Sophie Schmieg, senior staff cryptography engineer, published *"Quantum frontiers may be closer than they appear"* (blog.google). Google is "setting a timeline for post-quantum cryptography migration to 2029," reflecting progress in "hardware development, quantum error correction, and quantum factoring resource estimates."

Two elements matter commercially. First, Google explicitly reframed its threat model to prioritise post-quantum migration for authentication services, and recommended other engineering teams follow. Second, it treats encryption as already exposed — the threat "is relevant today with store-now-decrypt-later attacks" — while signatures are the future problem that must be solved before a quantum computer exists. Android 17 is integrating ML-DSA signature protection; Chrome and Google Cloud already support post-quantum key exchange.

Google has since reiterated the date in its research communications, referring to "our 2029 timeline" and naming Coinbase, the Stanford Institute for Blockchain Research and the Ethereum Foundation as collaborators (Google Research).

Cloudflare — April 2026, thirteen days later

Bas Westerbaan of Cloudflare Research published a roadmap targeting 2029 for full post-quantum security, **including authentication** (blog.cloudflare.com). Cloudflare reports more than 65% of human-initiated traffic on its network already uses post-quantum encryption, offered on all websites and APIs since 2022, and commits to delivering post-quantum upgrades on every plan at no additional cost — the same posture it took on universal SSL in 2014. The roadmap cites the Google and Oratomic papers by name, and references IBM Quantum Safe CTO Michael Osborne's assessment that quantum "moonshot attacks" on high-value targets cannot be ruled out as early as 2029.

Two organisations carrying a large share of global web traffic arrived at the same year, independently, within a fortnight. That is what turned one company's risk calculus into an industry benchmark.

Microsoft — June 30, 2026

Mark Russinovich, chief technology officer of Microsoft Azure, published *"Accelerating the quantum-safe timeline"* (Microsoft Security Blog).

> *"Advances in quantum research and development have shifted the risk horizon. We believe cryptographically relevant quantum computers could arrive sooner than previously expected — and the work required to prepare is significant so organizations need to start now."*
>
> — Mark Russinovich, CTO, Microsoft Azure

Microsoft is accelerating its Quantum Safe Program to transition critical products and services to post-quantum cryptography by 2029, and folding post-quantum requirements into the Secure Future Initiative — the same governance framework it applies to other critical security outcomes, with named ownership and measurable milestones. Its three engineering priorities are worth copying: TLS 1.3 negotiated by default on critical endpoints; crypto-agility for data at rest, with hard-coded algorithms eliminated; and modernised trust chains covering code signing, certificate issuance, key protection and update pipelines.

Russinovich also names the constraint most enterprises underestimate: "the hardest part isn't selecting post-quantum algorithms. It's understanding and updating where cryptography already exists across apps, services, networks, identities, certificates, and hardware." Microsoft's recommendation is **inventory first**.

One caution for anyone citing this: Microsoft says it is bringing the timeline forward but does not state a previous target date. The widely repeated "four years earlier" figure comes from third-party analysis, not from Microsoft.

Washington and Paris Made It Binding

Until June, every quantum deadline was a recommendation. Two governments changed that in eight days.

Executive Order 14412 — June 22, 2026

"Securing the Nation Against Advanced Cryptographic Attacks" was signed alongside a companion order, EO 14413, on quantum innovation (White House · Federal Register).

- **Dec. 31, 2030** — federal agencies must move their most sensitive systems to post-quantum encryption.
- **Dec. 31, 2031** — deadline for post-quantum authentication.

- **End of 2030** — federal contractors directed to comply with post-quantum FIPS, via the Federal Acquisition Regulation.
- Coordination assigned to OMB and the National Cyber Director; NIST works with NSA and CISA on standards.
- The order warns explicitly that foreign actors may already be collecting encrypted information with the intention of decrypting it later.

The commercial consequence is the contractor clause. A supplier to the U.S. government now has a dated cryptographic obligation regardless of its own risk assessment. Legal analyses from Covington and Sidley set out the scope; Cloudflare and Palo Alto Networks published implementation guidance (Cloudflare · Palo Alto Networks).

France — June 16, 2026

Speaking at the France Quantum conference at Station F in Paris, Samih Souissi, chief of staff of the national cybersecurity agency ANSSI, said the agency will **halt certification of security products lacking quantum-resistant encryption from 2027**, and that businesses should be purchasing only quantum-safe products by 2030 (Reuters).

Because ANSSI approval is a prerequisite for deployment across French government bodies and critical infrastructure, this is not guidance. It is a procurement gate. A product that cannot demonstrate quantum-safe encryption does not get certified, and without certification it does not get the contract. Souissi framed it as "not only a technical issue" but "a matter of governance, industrial planning, regulation, and sovereignty."

Bruce Schneier and The Quantum Insider both flagged the significance (Schneier on Security · The Quantum Insider). France is the first major jurisdiction to attach a commercial consequence to a quantum deadline.

The Skeptic Who Changed His Mind

The most consequential statement of 2026 did not come from a vendor.

Scott Aaronson holds the Schlumberger Centennial Chair at the University of Texas at Austin and directs its Center for Quantum Information. He spent two decades as quantum computing's most prominent deflationist — the researcher who reliably explained what quantum computers cannot do and pushed back on vendor claims. In late April, days after his election to the National Academy of Sciences, he wrote on his blog Shtetl-Optimized:

> *"Some of the most reputable people in quantum hardware and quantum error-correction — people whose judgment I trust more than my own on those topics — are now telling me that a fault-tolerant quantum computer able to break deployed cryptosystems ought to be possible by around 2029."*
>
> — Scott Aaronson, Shtetl-Optimized, April 2026

He framed the post explicitly as a warning to the security community, while conceding "I'm not a timing guy" and attributing the assessment to hardware specialists rather than his own analysis (scottaaronson.blog · summary). Aaronson sells no post-quantum products. That is precisely why his revision carries more evidentiary weight than any vendor announcement.

The useful dissent from inside the industry: Brian LaMacchia, who led Microsoft's post-quantum transition from 2015 to 2022 and now works at Farcaster Consulting Group, told Ars Technica that Google's date is "certainly a significant acceleration/tightening of the public transition timelines we've seen to date, and is accelerated over even what we've seen the US government ask for." He added: "The 2029 timeline is an aggressive speedup but raises the question of what's motivating them." Google did not specify.

What They Are Not Saying

Executives will encounter headlines claiming quantum computers will break encryption in 2029. That is not what any of the primary sources say, and the distinction is worth getting right before it reaches a board deck.

PQShield, which advises on quantum transition, put it plainly in April: neither Google nor Cloudflare is predicting that a cryptographically relevant quantum computer will exist by 2029. What they are saying is that **they can no longer confidently rule it out** (PQShield).

2029 is a migration deadline, not a doomsday date. Read correctly, that is the more alarming of the two claims. A prediction can be argued with. Three of the largest infrastructure operators on earth rebuilding their cryptographic stacks four years ahead of schedule, because they cannot rule out the risk, is a capital allocation decision — and it has already been made.

Why the Date May Not Matter

The strongest version of the case does not depend on 2029 being right.

Harvest now, decrypt later (HNDL) describes an adversary recording encrypted traffic today and storing it until a capable machine exists. Every authority in this article treats it as a present-tense risk: EO 14412 warns that foreign actors may already be collecting; Google states the threat to encryption "is relevant today"; Microsoft reports customers prioritising data with long confidentiality lifetimes; ANSSI cited HNDL directly in justifying its 2027 cutoff.

The chain of reasoning a board should be shown:

1. Data encrypted today with RSA or elliptic curve cryptography is being recorded today.
2. Migration is a multi-year engineering programme — Google, Microsoft and Cloudflare all say so, and they are better resourced than almost any customer.
3. Therefore, for any data with a confidentiality requirement extending beyond roughly 2029, the effective deadline **has already passed**.
4. If 2029 proves wrong and the real date is 2035, nothing is wasted. The deliverables — modern TLS, a cryptographic inventory, crypto-agility — pay for themselves on their own merits. Microsoft makes the point directly: organisations that begin with cryptographic discovery "consistently uncover existing gaps that require attention today, independent of quantum risk."

That asymmetry — **cheap if wrong, catastrophic if ignored** — is a stronger argument to a capital committee than any forecast.

The Bear Case

Serious people think this is overstated, and their objections belong in any honest briefing.

- **The physics may not cooperate.** Tim Palmer, a physicist at the University of Oxford, estimates quantum computers reach peak usefulness for factoring at roughly 1,000 qubits and will never scale to the million-plus required to break RSA-2048.
- **These are estimates, not demonstrations.** The resource papers assume sustained progress in qubit quality, error correction, thermal management and scale, with no showstoppers. Fireblocks' assessment is a fair statement of the gap: today's processors run in the hundreds to low thousands of physical qubits with error rates far too high for sustained fault-tolerant computation, and closing that gap requires breakthroughs "measured in years, not months."
- **Practitioner skepticism is vocal.** A representative response to the Ars Technica coverage: "more pointless quantum hype… It ain't happening in 2029; the qubit math doesn't add up."

- **Two of the loudest voices sell quantum computers.** Google and IBM both benefit from appearing to progress quickly. The counter: Cloudflare, Microsoft, ANSSI and the White House have no stake in quantum hardware, and moved anyway.
- **Mass retrospective decryption is implausible.** The sheer volume of global traffic makes an overnight collapse unlikely. The realistic threat model is targeted decryption of high-value archives — which is worse for some organisations and better for most.

The rebuttal that survives all of it: every objection attacks the date. None attacks the migration. NIST already deprecates RSA and ECC after 2030 and disallows them after 2035 whether or not a quantum computer ever appears. The work is mandatory; only the schedule is in dispute.

What Boards Are Being Told to Do

Drawn from Microsoft's and PQShield's published guidance rather than invented.

1. **Assign ownership.** Name an accountable executive, scope and milestones for a multi-year cryptographic transition. Microsoft folded this into the same governance framework it uses for other critical security outcomes; that is the model.
2. **Inventory before you migrate.** Build a living catalogue of every place public-key cryptography appears — TLS, code signing, API authentication, certificates, hardware, third-party dependencies. You cannot migrate what you have not mapped, and this is where most programmes stall.
3. **Triage by data lifetime, not system criticality.** Anything with a confidentiality requirement past roughly 2030 is already exposed to HNDL and goes first.
4. **Get to TLS 1.3.** It is the prerequisite for hybrid and post-quantum key exchange, and the cheapest item on this list.
5. **Build crypto-agility.** Move cryptographic settings out of application code, standardise key management and rotation, eliminate hard-coded algorithms. The objective is that the next transition is a configuration change rather than a rewrite — and there will be a next transition.
6. **Prioritise authentication, not just encryption.** This is the substantive shift in both Google's and Cloudflare's announcements. Encryption is already partly protected by deployed hybrid key exchange. Signatures, certificates and identity infrastructure are slower to fix, and a forged signature cannot be repaired after the fact.
7. **Plan for the certificate collision.** Jason Soroko of Sectigo notes that 2029 is also the year the CA/Browser Forum's 47-day maximum TLS certificate lifespan takes full effect — a 12-fold increase in renewal frequency. Two cryptographic transitions land in the same year, and both demand the same underlying capability: automated, rapid rotation.
8. **Set your own Q-Day.** Per PQShield: be explicit about your risk tolerance rather than choosing it by default through inaction.

Sources

Primary — government

- Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," June 22, 2026 — https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/
- Federal Register, Vol. 91, No. 121, June 25, 2026 (official text) — https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks
- Reuters, "France to stop certifying products without quantum-safe encryption," June 16, 2026 — https://www.reuters.com/legal/litigation/france-stop-certifying-products-without-quantum-safe-encryption-2026-06-16/
- NIST IR 8547 — quantum-vulnerable algorithms deprecated after 2030, disallowed after 2035. NSA CNSA 2.0 — approximately 2030–2033 for national security systems.

Primary — corporate

- Google, "Quantum frontiers may be closer than they appear," Adkins & Schmieg, March 25, 2026 — https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/
- Microsoft, "Accelerating the quantum-safe timeline," Mark Russinovich, June 30, 2026 — https://www.microsoft.com/en-us/security/blog/2026/06/30/microsoft-advances-quantum-safe-security-as-the-risk-timeline-shifts/
- Cloudflare post-quantum roadmap, Bas Westerbaan, April 2026 — https://blog.cloudflare.com/post-quantum-roadmap/
- Cloudflare on EO 14412 — https://blog.cloudflare.com/post-quantum-eo-2026/
- Google Security Blog, "Tracking the Cost of Quantum Factoring," May 2025 — https://security.googleblog.com/2025/05/tracking-cost-of-quantum-factori.html
- Google, post-quantum cryptography in Android, March 2026 — http://security.googleblog.com/2026/03/post-quantum-cryptography-in-android.html
- Google Research, "Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly" — https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/

Research

- Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv:2505.15917 — https://arxiv.org/abs/2505.15917
- Gidney & Ekerå (2019), arXiv:1905.09749 — https://arxiv.org/pdf/1905.09749
- Google Research listing for the 2025 paper — https://research.google/pubs/how-to-factor-2048-bit-rsa-integers-with-less-than-a-million-noisy-qubits/
- "Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities," arXiv:2603.28846, March 30, 2026 — https://quantumai.google/static/site-assets/downloads/cryptocurrency-whitepaper.pdf

Expert assessment

- Scott Aaronson, Shtetl-Optimized — https://scottaaronson.blog/ · summary: https://postquantum.com/security-pqc/aaronson-quantum-warning-nas/
- PQShield, "On Quantum Timelines: What Does '2029' Actually Mean?" — https://pqshield.com/on-quantum-timelines-what-does-2029-actually-mean/
- PQShield on Microsoft's acceleration — https://pqshield.com/microsoft-accelerates-quantum-safe-timeline-for-adoption-by-2029/
- Brian LaMacchia (Farcaster Consulting Group), quoted in Ars Technica. Michele Mosca (evolutionQ, University of Waterloo), quoted by CNN. Michael Osborne (CTO, IBM Quantum Safe), cited by Cloudflare. Justin Drake (Ethereum Foundation) — approximately 10% chance of Q-Day by 2032. Tim Palmer (University of Oxford), quoted in Computing.

Press coverage

- Ars Technica, Dan Goodin, "Google bumps up Q Day estimate to 2029, far sooner than previously thought," March 25, 2026.
- CNN, "Quantum computing threatens to unleash a cybersecurity crisis," May 17, 2026 — https://www.cnn.com/2026/05/17/science/quantum-computing-cybersecurity-q-day

- Dark Reading, March 27, 2026 — https://www.darkreading.com/application-security/google-2029-deadline-quantum-safe-cryptography
- Infosecurity Magazine — https://www.infosecurity-magazine.com/news/quantum-encryption-q-day-closer/
- The Hacker News, July 2026 — https://thehackernews.com/2026/07/microsoft-accelerates-post-quantum.html
- Redmond Magazine, July 1, 2026 — https://redmondmag.com/articles/2026/07/microsoft-moves-up-quantum-safe-security-timeline.aspx
- The Quantum Insider, July 1, 2026 — https://thequantuminsider.com/2026/07/01/microsoft-moves-up-quantum-safe-security-deadline-to-2029/
- The Quantum Insider, "Q-Day Just Got Closer," March 31, 2026 — https://thequantuminsider.com/2026/03/31/q-day-just-got-closer-three-papers-in-three-months-are-rewriting-the-quantum-threat-timeline/
- The New Stack, "Microsoft, Google and Cloudflare just made 2029 the new quantum deadline" — https://thenewstack.io/post-quantum-cryptography-deadline-2029/
- TechSpot, March 27, 2026 (carries the LaMacchia quote) — https://www.techspot.com/news/111856-google-sets-2029-deadline-quantum-safe-encryption-years.html
- Keyfactor, "Google Just Moved the Q-Day Deadline to 2029" — https://www.keyfactor.com/blog/google-just-moved-the-q-day-deadline-to-2029-heres-what-that-means-for-you/
- SecureWorld / Sectigo on the 2029 certificate-lifespan collision — https://www.secureworld.io/industry-news/google-2029-deadline-post-quantum-cryptography-migration
- Schneier on Security — https://www.schneier.com/blog/archives/2026/07/france-to-stop-certifying-non-quantum-safe-encryption.html
- Covington, Inside Privacy — https://www.insideprivacy.com/cybersecurity-2/trump-administration-releases-two-executive-orders-on-quantum/ · Sidley, Data Matters — https://datamatters.sidley.com/2026/07/01/white-house-issues-executive-orders-on-quantum-innovation-and-security/
- Palo Alto Networks — https://www.paloaltonetworks.com/blog/2026/06/new-executive-order-accelerates-post-quantum-readiness-amid-the-cryptographic-reset/ · Information Age / ACS — https://ia.acs.org.au/article/2026/google--cloudflare-want-post-quantum-cryptography-by-2029.html
- PostQuantum.com on Cloudflare — https://postquantum.com/security-pqc/cloudflare-pqc-2029/

All citations verified against primary sources as of July 30, 2026. Figures for qubit counts are published resource estimates, not demonstrated attacks; no machine at the scale described in these papers is known to exist.

Transformativ IP

info@TransformativIP.ai