

Quantum computing & US critical infrastructure

DR. BRIAN ROBERT CALLAHAN

INFRAGARD NJ 2026 ANNUAL INDUSTRY UPDATE

SEPT. 18, 2026



MONMOUTH
UNIVERSITY

CYBERSECURITY
RESEARCH CENTER



IBM

IBM Quantum
System One

Some terms up front

- ▶ Quantum computing
 - ▶ *A new paradigm of computing that uses quantum phenomenon to computer rather than transistors*
- ▶ Classical computers
 - ▶ *The computers you are used to: laptops, desktops, cell phone, etc.*
- ▶ Q-Day
 - ▶ *The hypothetical date in which quantum computers can trivially crack modern cryptography*
- ▶ Post-Quantum Cryptography (PQC)
 - ▶ *Cryptographic algorithms and standards that cannot be easily broken by classical or quantum computers (we hope!)*

If you leave with nothing else...

- ▶ The hardware is arriving later than the hype claims. But the policy deadlines have already arrived, and the data is already being stolen. Critical infrastructure is uniquely exposed because its equipment lives for quite a long time, its cryptography is buried in firmware nobody has inventoried, and its adversaries are already inside the networks. The migration is a decade-long engineering project that must start now, and the same quantum toolchain that threatens the grid is also one of the best new tools for running it.

Who am I?

Towards Practical Quantum Kernels for Network Intrusion Detection

Mary L. Cotrupi
Rensselaer Polytechnic Institute

Brian R. Callahan
Monmouth University

DOI: <https://doi.org/10.1609/aaaiss.v7i1.36903>



Hardware Robustness of Quantum Machine Learning Kernels for Malware Detection

Mary L. Cotrupi¹, Allison Aurilio², Sean Sanpietro³, Fabiana Torres⁴, Anwita Kasturi¹, Quinn Colognato¹, Brian Robert Callahan⁴

¹Dept. of Computer Science, Rensselaer Polytechnic Institute, Troy, NY 12180-3590 USA

²Dept. of Electrical and Computer Engineering, The College of New Jersey, 2000 Pennington Road, Ewing, NJ 08618-1100 USA

³Dept. of Computer Science, Misericordia University, 301 Lake Street, Dallas, PA 18612-7752 USA

⁴Dept. of Computer Science and Software Engineering, Monmouth University, 400 Cedar Avenue, West Long Branch, NJ 07764-1828 USA

cotrum@rpi.edu, aurilia2@tcnj.edu, ssanpiet@misericordia.edu, s1378769@monmouth.edu, kastua@rpi.edu, cologq@rpi.edu, bcallaha@monmouth.edu

Quantum Preprocessing for Internet of Things Edge Computing Security Devices

Publisher: IEEE

[Cite This](#)

[PDF](#)

[Tiffany Cheng](#) ; [Shoshana Sugerman](#) ; [Colin Farley](#) ; [Brian Robert Callahan](#) All Authors

2025 Journal of The Colloquium for Information Systems Security Education, Volume 12, No. 1, Spring 2025

Multidisciplinary Quantum Cybersecurity Research for the Undergraduate Laboratory



The grid doesn't get a second
chance

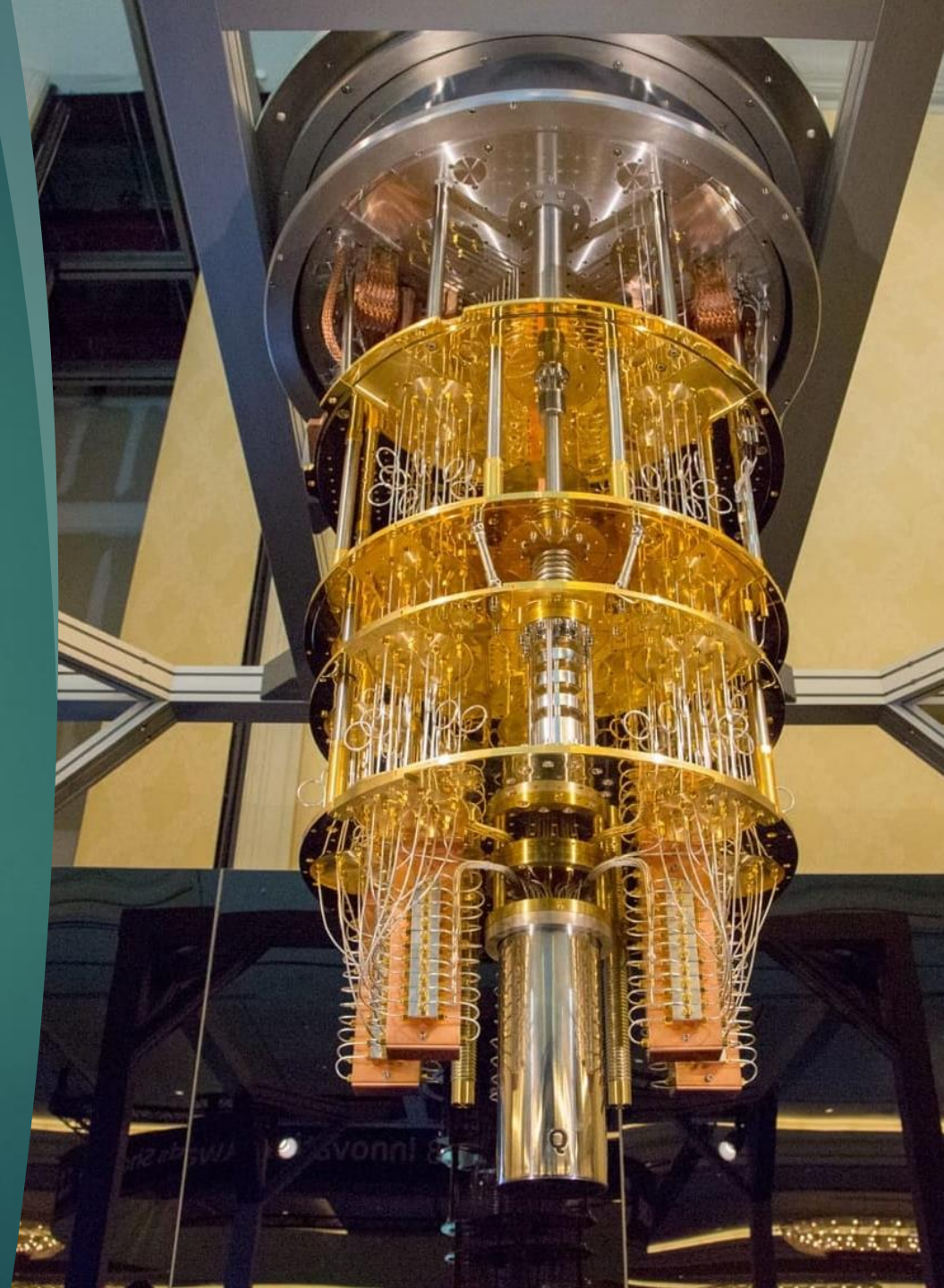
We have already decided...

- ▶ Which part of America's infrastructure are most exposed to quantum computers
- ▶ You can see it here too. CISA has already ranked all 55 National Critical Functions as high, medium, or low priority for post-quantum migration:
https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf
- ▶ This was back in 2022
- ▶ ...We just haven't fixed them yet

The Machine

What is a quantum computer, anyway?

- ▶ Is it a faster computer?
 - ▶ Yes but no...
- ▶ Is it more more capable computer?
 - ▶ Yes but no...
- ▶ It is a different paradigm of computing
 - ▶ Yes, absolutely. Quantum exploits superposition and entanglement for specific problem classes
- ▶ Is it general purpose in the way classical computers are?
 - ▶ No, not in that sense



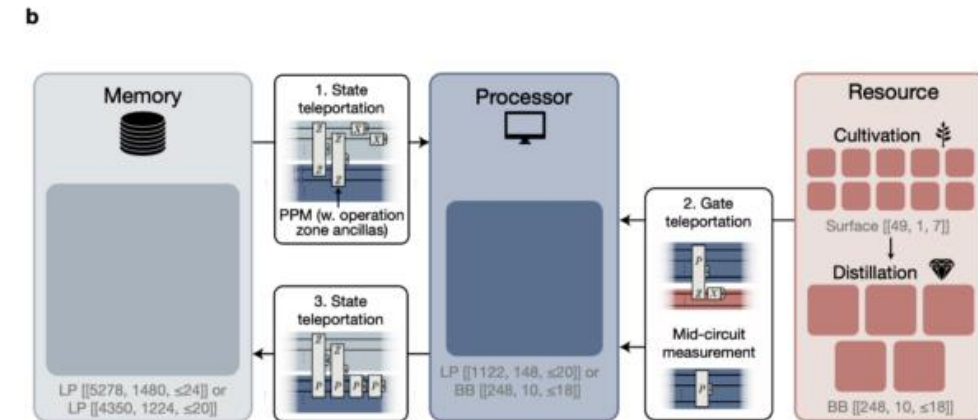
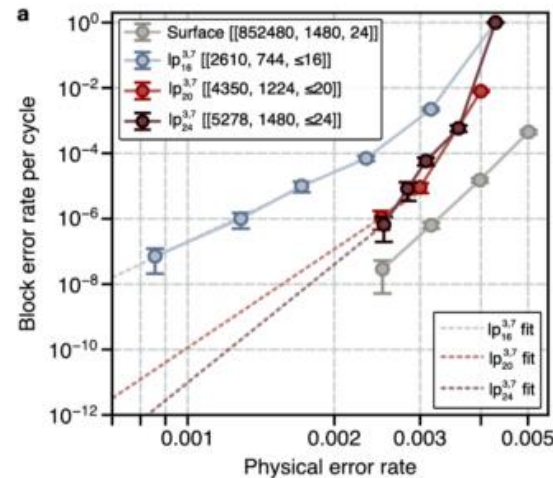
What's the latest in quantum in 2026?

- ▶ Previously, it was number of qubits
- ▶ Now, it is stability, error correction, and long-duration logical coherence
- ▶ The current “era” of quantum is called NISQ: Noisy Intermediate Scale Quantum
- ▶ If you believe the hype, we are currently moving past the NISQ era into being able to produce fault-tolerant quantum chips
- ▶ This will all but eliminate one of the core physical constraints of today's currently existing quantum computers

What does
this mean,
realistically,
for us

<https://arxiv.org/pdf/2603.28627>

- ▶ Q-Day is coming and it will probably be a whole lot less expensive than we thought.
- ▶ Current research believes Shor's algorithm is possible with only 10,000 qubit
- ▶ ECC-256 breakable in about 10 days



Google is also getting in on breaking ECC-256

- ▶ <https://quantumai.google/static/site-assets/downloads/cryptocurrency-whitepaper.pdf>
- ▶ Claims to be able to crack the public key in a bitcoin address in under 10 minutes, with 20 times fewer resources than what was achieved 20 years prior
- ▶ Less than 1,500 logical qubits (which is about 500,000 physical qubits)

RSA-2048 isn't safe either

- ▶ In 2012, about 1 billion qubits were estimated to be needed to crack RSA-2048
- ▶ In 2019, that number fell to 20 million
- ▶ In 2025, fell even further to 1 million
- ▶ <https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2026/q-day-quantum-threat.pdf>

And we're building these things more powerfully by the day

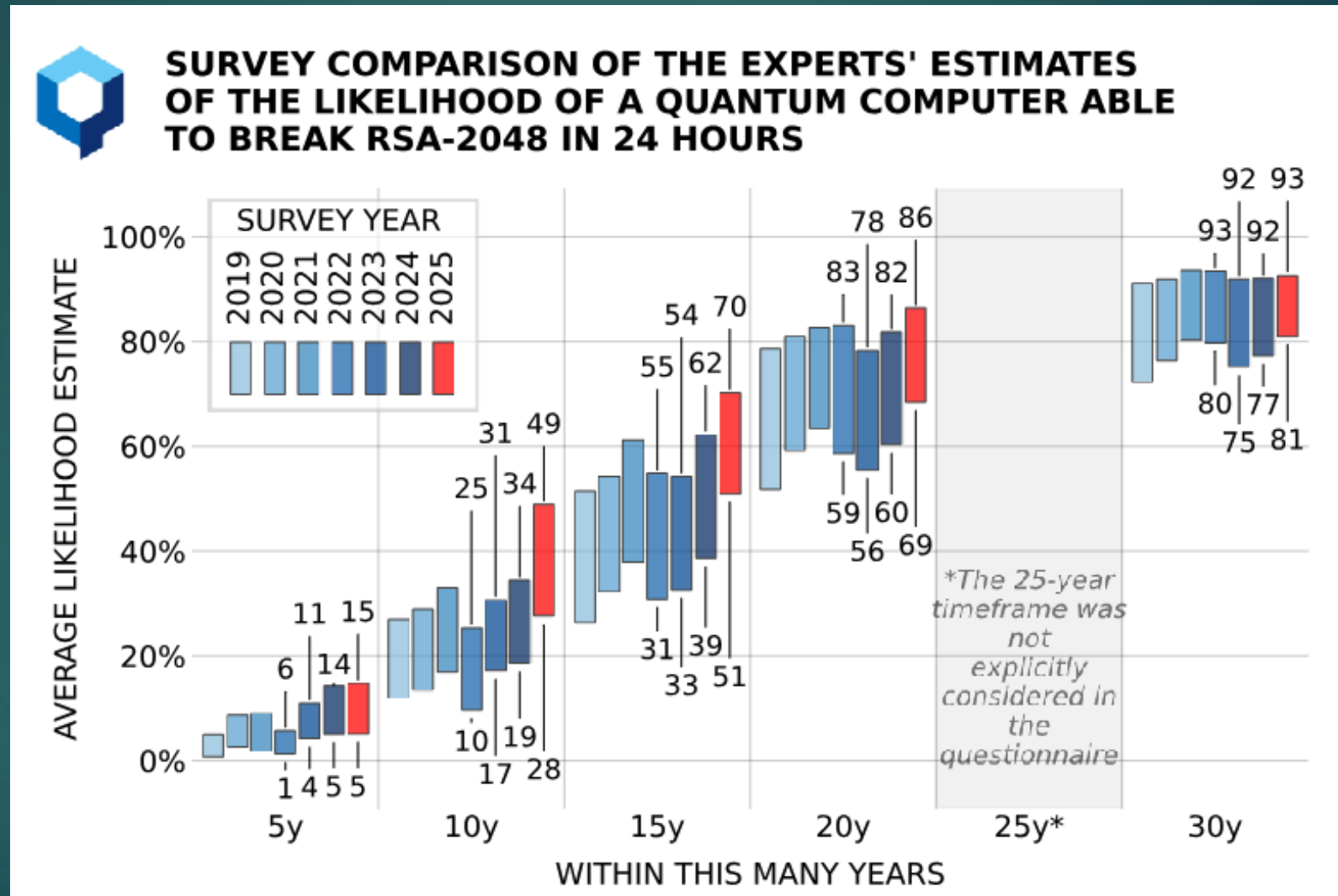
- ▶ IBM's roadmap for 2026 was to have a quantum chip that could support accurate observable estimation for circuits with more than 7,500 two-qubit gates by the end of 2026.
- ▶ They have already released the chip that does it: Nighthawk r2
- ▶ And it runs 25 times faster than the previous generation of quantum chips
- ▶ <https://www.ibm.com/quantum/blog/nighthawk-r2>



Quantum is no longer a toy

IT HAS A REAL ROADMAP WHOSE MILESTONES ARE BEING BEATEN

So what's realistic?



Can we come up with a date for Q-Day?

- ▶ Consensus is that Q-Day falls in the 2030s (or later)
- ▶ Not really possible to come up with an exact date
- ▶ Feels like the date keeps moving up with each new hardware and algorithmic breakthrough...

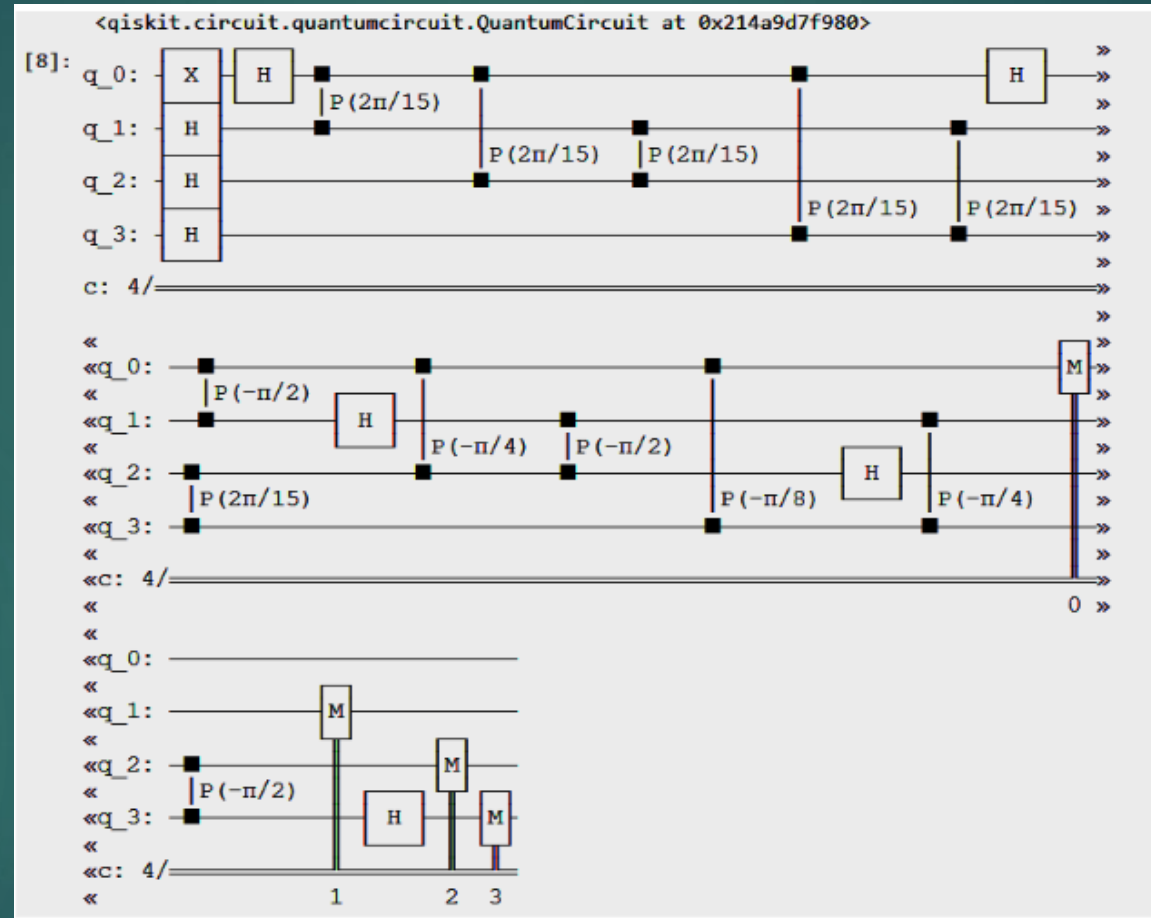
Better question: Does having a date for Q-Day matter?

- ▶ **No**
- ▶ Google is setting their own timeline for PQC migration to be no later than 2029: <https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/>
- ▶ If even Google needs 3 years to do it, how much time does critical infrastructure need?

Now, here's why this is a critical infrastructure story and not just a cryptography story...

The Threat

Shor's algorithm



<https://doi.org/10.53735/cisse.v12i1.206>

Harvest now, decrypt later (HNDL)

- ▶ It's happening now
- ▶ Everyone is talking about it now
(<https://www.federalreserve.gov/econres/feds/files/2025093pap.pdf>)
- ▶ It is an active threat
- ▶ Nation-state actors are doing it ([https://d3cconsulting.com/harvest-now-decrypt-later/#Who Is Behind Harvest Now Decrypt Later Attacks](https://d3cconsulting.com/harvest-now-decrypt-later/#Who%20Is%20Behind%20Harvest%20Now%20Decrypt%20Later%20Attacks))
- ▶ **They are already stealing from hospitals and banks, and other critical infrastructure**
- ▶ <https://labs.cloudsecurityalliance.org/research/ai-infrastructure-post-quantum-harvest-now-decrypt-later-v1/>

Why infrastructure is uniquely exposed

- ▶ From CISA:
“NCFs that depend on data confidentiality over long time frames are uniquely vulnerable to quantum challenges, including catch-and-exploit campaigns in which adversaries capture data that has been encrypted using current encryption algorithms and hold on to such data with the intention of decrypting it when a quantum computer capable of breaking the encryption is available.”
(https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf)
- ▶ Water, power, healthcare, and telecommunications are expected to face even greater risk (<https://securitybrief.ca/story/quantum-threats-to-drive-overhaul-of-cybersecurity-by-2026>)

Why infrastructure is uniquely exposed

- ▶ GAO has warned adversaries could use quantum computers to disrupt the availability of essential services
(<https://www.gao.gov/assets/gao-25-107703.pdf>)

The asset lifecycle problem

- ▶ WEF makes this clear for the energy sector: HNDL risks make early planning for your long-lived assets essential
(https://reports.weforum.org/docs/WEF_Quantum_for_Energy_and_Utilities_2026.pdf)

And nation-state adversaries are already in the systems

- ▶ Volt Typhoon (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>)
- ▶ And Salt Typhoon (<https://axis-intelligence.com/critical-infrastructure-cyber-attacks-statistics/>)

The Clock

The policy timeline already exists

- ▶ May 2022: National Security Memorandum 10 sets a 2035 federal migration target
- ▶ December 2022: Quantum Computing Cybersecurity Preparedness Act reinforces it and directs OMB to develop a strategy
- ▶ August 2024: NIST finalizes the first three post-quantum standards

<https://openssl-corporation.org/blog/post-quantum-cryptography-now-has-deadlines.html>

The NIST standards

- ▶ FIPS 203: ML-KEM (key encapsulation)
- ▶ FIPS 204: ML-DSA (digital signatures)
- ▶ FIPS 205: SLH-DSA (stateless hash-based signatures)
- ▶ NIST says they can be implemented **now** (<https://www.nist.gov/pqc>)

Deprecation timelines

- ▶ Under NIST IR 8547, RSA and elliptic curve cryptography (ECC) are scheduled for **deprecation by 2030** and **disallowance by 2035** (<https://openssl-corporation.org/blog/post-quantum-cryptography-now-has-deadlines.html#:~:text=Every%20mandate%20above,set%20is%20settled>)
- ▶ *A lot of vendor marketing claims "NIST mandates PQC by 2026." That is false. The binding dates are 2030/2035. Don't believe everything you read on the Internet! 😊*

NSA CNSA 2.0: the most specific timeline

- ▶ Announced September 2022; replaces CNSA 1.0 (RSA/ECC/DH)
- ▶ Requires only the highest NIST security levels: ML-KEM-1024 and ML-DSA-87; lower parameter sets are not permitted for National Security Systems
- ▶ January 1, 2027: acquisition gate for new NSS
- ▶ Operating systems: support and prefer by 2027, exclusive use by 2033
- ▶ Software/firmware signing: exclusive use by 2030
- ▶ Full transition by December 31, **2033**

What's happening right now?

- ▶ On 22 June 2026, two executive orders were signed:
 - ▶ "Ushering in the Next Frontier of Quantum Innovation" establishes the QC-ADDs effort (Quantum Computer for Application Development and Discovery Science), with the goal of a quantum computer enabling meaningful scientific breakthroughs by 2028
 - ▶ "Securing the Nation Against Advanced Cryptographic Attacks" accelerates PQC adoption across government, and notably directs CISA, with NIST, to publish guidance on minimum elements for a "cryptographic bill of materials" to enable automated assessment of cryptographic assets in hardware and software

<https://www.klgates.com/thought-leadership/Preparing-for-Q-Day-New-Executive-Orders-Address-Quantum-Innovation-and-Post-Quantum-Cryptography-6-26-2026>

Your deadlines

KEY DEADLINES

The two executive orders establish a series of implementation deadlines. Organizations monitoring federal quantum policy should take note of the following milestones:

Deadline	Requirement
30 days	Each agency must designate a PQC-migration lead
90 days	OMB must issue guidance requiring agencies to review HVA inventories and develop PQC transition plans
180 days	NIST must initiate a PQC-migration pilot project (completion by 31 December 2027)
180 days	NQS must be updated
180 days	FAR Council must publish a proposed rule requiring covered contractors to comply with FIPS/PQC standards by 31 December 2030
270 days	CISA must release public guidance on minimum elements for a cryptographic bill of materials
270 days	FAR Council must publish a proposed rule on contractor-vulnerability disclosure programs incorporating cryptographic vulnerabilities
31 December 2030	All HVAs and high-impact systems must use PQC for key establishment
31 December 2031	All HVAs and high-impact systems must use PQC for digital signatures

<https://www.klgates.com/thought-leadership/Preparing-for-Q-Day-New-Executive-Orders-Address-Quantum-Innovation-and-Post-Quantum-Cryptography-6-26-202>

Important notes

- ▶ The federal government is using procurement as the enforcement mechanism. If you sell to the government, PQC compliance becomes a contract term by 2030
- ▶ OMB's M-26-15 identifies the foundation of the whole effort as "a dynamic, continuously updated inventory of all cryptographic assets," with automation recommended wherever possible
- ▶ It also directs risk-based prioritization: HVAs, high-impact systems, and any system holding data expected to remain mission-sensitive in 2030

Where the strategy is still incomplete

- ▶ GAO found the federal quantum-cybersecurity strategy documents did not fully define objectives or activities for encouraging all sectors — including critical infrastructure — to migrate to PQC
- ▶ GAO recommended the Office of the National Cyber Director lead coordination of the national strategy
- ▶ GAO's March 2026 report recommends OSTP update the national quantum strategy
- ▶ *The federal government has given itself deadlines. It has not yet given industry a roadmap. That gap is your organization's problem to solve.*

<https://www.gao.gov/products/gao-25-108590>

<https://www.gao.gov/products/gao-26-107759>

And Congress is moving too

- ▶ August 2026: Senators Chris Coons (D-DE) and Mike Rounds (R-SD) introduced the bipartisan Quantum-GUARD Act (Quantum Grid Utility Assurance and Resilient Defense Act of 2026)
- ▶ It directs FERC to consider quantum cybersecurity risks within its grid reliability authority; establish a DOE CESER collaborative testing environment for PQC adoption; and require DOE CESER to study quantum cyber risks to the bulk electric power system, including both IT and OT vulnerabilities



The Opportunity

(THIS IS WHERE WE STOP BEING DOOM-Y AND START BEING OPTIMISTIC)

(EVERYONE SMILE AND LAUGH HERE: THE GOOD OUTWEIGHS THE BAD)

Quantum is a grid tool too!

- ▶ WEF's *Quantum for Energy and Utilities* report (2026): quantum computing, sensing, and communication are moving from research into early pilots in the energy sector as tools for specific, hard problems
- ▶ The earliest opportunities: hybrid quantum-classical optimization, emerging sensing applications, and post-quantum cybersecurity upgrades

https://reports.weforum.org/docs/WEF_Quantum_for_Energy_and_Utillities_2026.pdf

Three waves of quantum defense

- ▶ **Near-term:** decision optimization in operations and markets
- ▶ **Mid-term:** system planning and control, as grids and variable generation scale up
- ▶ **Longer-horizon:** R&D, once fully fault-tolerant machines arrive

Your opportunities to use quantum as a tool for defense



Area	Applications
Transmission	Large-scale optimization of high-voltage grid flows, cross-border trading, fault/stress detection, QKD for grid communication
Distribution	Local optimization of distributed energy resources, EV charging scheduling, anomaly detection, secure smart meters
Storage	Simulating new battery chemistries, catalyst design for hydrogen, monitoring battery-farm degradation
Water/wastewater	Optimizing desalination and treatment, smart water distribution, contaminant/micro-leak detection
Nuclear	Reactor design, materials discovery, radiation detection, quantum-safe encryption

And yes, it's really happening now

- ▶ Aramco used D-Wave's hybrid system to sharpen seismic imaging (https://www.sec.gov/Archives/edgar/data/1907982/000190798224000072/d-wave_aramcoexpressxrlsxfi.htm)
- ▶ Repsol Sinopec tested QLM's quantum lidar for better detection of small/intermittent methane leaks (https://qlmtec.com/case_studies/652e55927be17ef72ec1e1f2)
- ▶ Exail's absolute quantum gravimeter for drift-free, long-duration reservoir monitoring (<https://www.exail.com/product/quantum-gravimeters>)
- ▶ EDF / Pasqal implemented a quantum-annealing schedule optimizer for EV charging (<https://www.pasqal.com/newsroom/edf-leverages-pasqal-to-successfully-run-energy-demand-forecasts-for-electric-vehicle-smart-charging/>)
- ▶ ExxonMobil / IBM researched maritime inventory routing via hybrid quantum optimization (<https://www.ibm.com/case-studies/exxonmobil>)

Quantum sensing: the underrated near-term winner

- ▶ Quantum sensing improves precision and stability of radiation and environmental monitoring, and quantum-safe communication protects operational data against future cryptographic threats
- ▶ ORNL's Quantum Communications and Networking Group develops next-generation quantum communication to create secure, resilient networks for US critical infrastructure with a focus on the power grid and metropolitan-scale quantum networks
(<https://www.ornl.gov/group/quantum-communications-networking>)

And you're already funded!

- ▶ NSF Project Triad is a first-of-its-kind initiative to integrate quantum sensing, quantum networking, and quantum computing into a single operational system so that we can move quantum out of the lab into real-world use across safety, healthcare, energy, and manufacturing (<https://www.nsf.gov/news/nsf-launches-project-triad-advance-quantum-technology-real>)
- ▶ Fiber Connect 2026 showed quantum converging with fiber, edge, security, and data-center infrastructure as operators prepare for distributed quantum networking and Q-Day cybersecurity (<https://www.datacenterfrontier.com/design/article/55379465/fiber-connect-2026-puts-quantum-on-the-infrastructure-map>)

The Playbook

There are difficulties...

- ▶ The most basic challenge is determining who owns the migration process at the organizational level
- ▶ There is no universally accepted implementation roadmap or timeline; your organization must decide what to prioritize, how to balance competing risks, and how to fund multi-year work
- ▶ And PQC work competes with more immediate, more easily quantifiable threats while modifying cryptographic systems introduces its own operational disruption risk...

<https://www.rstreet.org/research/post-quantum-cryptography-migration-in-the-united-states-managing-risk-and-advancing-cyber-readiness-in-critical-infrastructure/>

...but five steps is all it takes (IPASC, no, I'm not good at making catchy names)

- ▶ **Inventory:** build a dynamic, continuously updated cryptographic asset inventory; automate mapping of the cryptographic environment and its dependencies
- ▶ **Prioritize:** by HNDL exposure; assess org-level HNDL risk; systems storing or transmitting long-term-sensitive data need the highest levels even if immediate decryption is impossible
- ▶ **Adopt:** cryptographic agility; plan for CBOM-style visibility so you can swap algorithms without replacing hardware
- ▶ **Start:** Now is the time to start; CISA's guidance is explicit: start preparing now, and don't wait until adversaries have quantum computers to act
- ▶ **Coordinate:** CISA, NSA, and NIST jointly published migration guidance precisely so that critical infrastructure doesn't each solve this alone

What to go home with

- ▶ The hardware is slower than the hype, but the deadlines are already real (2030 key establishment, 2031 signatures, 2033 NSS, 2035 full)
- ▶ The data is already being harvested
- ▶ The same technology is a tool for the grid, not just a threat to it
- ▶ IPASC (no, I'm still not good at making catchy names, but if we all start using it, maybe it'll become a thing 😊)

We will succeed

- ▶ *Quantum computing will change critical infrastructure twice: once when it breaks cryptography, and again when it helps run critical infrastructure. The first change is already in progress. Let's make sure we're well on our way to the second when the first arrives.*

Thanks (Connect with me on
LinkedIn) (And enjoy lunch 😊)

