G1VE TECHNOLOGIES

# The Quantum Clock Is Already Running: Why Critical Infrastructure Cannot Wait to Migrate to Post-Quantum Defenses

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

May 17, 2026

**Original source**

https://www.linkedin.com/pulse/quantum-clock-already-running-why-critical-cannot-w-b--bssze/

## I. The Quietest National Security Risk Is Also The Most Strategic

Cyber threats tend to be loud. Breaches, ransomware events, infrastructure intrusions, and supply-chain compromises generate headlines that force boards and agencies to react. But the most strategically important cyber risk in the United States right now is one of the quietest. It is the slow but unmistakable arrival of quantum-enabled cryptographic risk, and the parallel pressure to migrate the country's most sensitive systems to post-quantum cryptography (PQC) before that risk becomes catastrophic.

In April, the U.S. Senate Committee on Commerce, Science, and Transportation Democratic Members advanced the National Quantum Initiative Reauthorization Act with several amendments aimed at accelerating near-term applications, expanding manufacturing, and — most importantly for infrastructure leaders — pushing forward a National Quantum Cybersecurity Migration Strategy. The strategy would direct the White House Office of Science and Technology Policy to coordinate development of a national approach to preparing federal systems for the cybersecurity threats posed by advancing quantum capabilities.

That is the quiet announcement that deserves to be loud. Because the cryptographic foundations underneath the U.S. economy and national security stack are not going to migrate themselves.

## II. The Threat Is Asymmetric, Patient, And Pre-Positioned

The most dangerous part of the quantum risk is not the day a fault-tolerant quantum computer becomes operational at scale. The most dangerous part is what adversaries are doing right now. The widely understood concept of "harvest now, decrypt later" is no longer a theoretical concern. Adversaries are already capable of capturing encrypted traffic, sensitive datasets, intellectual property, financial flows, infrastructure communications, and government records — and storing them for future decryption once quantum capability matures.

That means the breach is happening now, even if the decryption arrives later. For national security planners, this is one of the rare cases where the strategic risk timeline runs backwards: damage that will appear in the future is already being prepared in the present. Waiting for a clear public sign that quantum is operational before migrating to PQC is not a defensible posture. It is a planning failure.

The Senate amendments folded into the NQIA reauthorization recognize this reality. The National Quantum Cybersecurity Migration Strategy is meant to give the federal government a coordinated national approach — not just agency-by-agency improvisation.

## III. Critical Infrastructure Is The Most Exposed Surface

Federal networks matter. But the largest concentration of quantum-relevant exposure sits in critical infrastructure: energy, water, telecom, finance, transportation, healthcare, defense industrial base, and operational technology environments tied to physical processes. These sectors use cryptography across an enormous range of functions — identity, authentication,

signaling, transactions, control systems, vendor connections, software updates, telemetry, and command-and-control links.

That is where the migration problem becomes especially difficult. Infrastructure environments often run on long-lifecycle equipment, contractor-managed devices, legacy operating systems, vendor-specific cryptographic libraries, and embedded systems that cannot be patched quickly. They were not built with cryptographic agility in mind. Migrating them to post-quantum standards is not a one-quarter project. It is a multi-year program that requires inventory, planning, vendor coordination, testing, and disciplined execution.

The longer that work is delayed, the worse the eventual transition will be.

## IV. The Threat Picture Is Sharper Because The Adversary Is Already Operational

The strategic urgency of post-quantum migration is reinforced by what adversaries are already doing in the conventional cyber domain. In April, U.S. authorities warned that Iran-aligned hackers had exploited and disrupted operational technology control systems across multiple U.S. critical-infrastructure sectors, targeting Rockwell Automation Allen-Bradley PLCs used in water, energy, and government services. The actors manipulated HMI and SCADA data and project files, in some cases causing operational disruption and financial loss.

This is not unrelated to the quantum issue. It tells us two things at once. First, adversaries are already willing to attack infrastructure for asymmetric effect. Second, the infrastructure environments most exposed to OT-based intrusions today are also the environments least equipped to manage a complex cryptographic transition tomorrow. If a sector cannot keep its PLCs off the open internet, it will struggle to manage a coordinated PQC migration across vendors, devices, and legacy systems.

The OT advisory is therefore a sneak preview of the quantum migration challenge. If the institution is not disciplined enough to maintain hygiene in today's threat environment, it will not magically become disciplined enough to handle a more complex cryptographic transition during a more contested global environment.

## V. The Defense Ecosystem Is Also Signaling The Cryptographic Shift

Looking just at federal cyber strategy makes this even clearer. The Trump administration's national cyber strategy, released in March, included quantum computing and post-quantum cryptography explicitly among its critical and emerging technology priorities, alongside AI-enabled cyber defense for federal networks. The strategy framed the move as part of sustaining U.S. superiority in critical and emerging technologies. That is not throwaway language. It is policy direction.

In parallel, the National Cyber Director publicly said additional cybersecurity executive orders are expected "relatively soon." That kind of signaling typically precedes implementation requirements, particularly for federal networks and critical infrastructure operators.

For infrastructure leaders, that means the policy environment is converging on a clear message: cryptographic modernization is no longer optional, and post-quantum readiness will be evaluated against a national standard, not local discretion.

## VI. The Institutional Capacity Gap Is Real

While the strategic direction is improving, the operational capacity to execute is uneven. In April, Cybersecurity and Infrastructure Security Agency 's acting director told lawmakers that resources to detect and counter cyber threats were "more limited than I would like." He noted that many preparatory activities and routine outreach the agency would normally conduct were not possible during ongoing DHS funding disruptions. The same period brought additional FY27 proposals affecting workforce development, stakeholder engagement, and parts of infrastructure protection.

That matters because PQC migration is not just a technical change. It is a national coordination effort. It requires guidance, outreach, sector-specific support, exercises, vendor coordination, and ongoing technical assistance. If the federal connective tissue weakens precisely as the migration challenge intensifies, then the country risks creating a structural delay in cryptographic readiness.

The lesson for infrastructure executives is simple: do not assume the federal government will catch you. The mature institutions will move first, regardless of how supportive the policy environment looks on any given week.

## VII. Mythos And The OT Exclusion Expose Another Dimension Of Rsk

Another quiet signal from May should also be read in this context. Reporting indicated that operational technology providers and their industry groups felt excluded from the initial rollout of Anthropic 's Mythos Preview model under Project Glasswing, despite the fact that OT environments embedded in critical infrastructure are widely targeted by adversaries. American Water , one of the country's largest regulated water utilities, was reportedly among those engaging the Office of the National Cyber Director about Mythos and broader AI-cybersecurity threats.

That story is important not because Mythos is the answer to PQC challenges, but because it shows a pattern. The most exposed segments of critical infrastructure — water, energy, transportation, manufacturing — often have the least leverage when frontier capabilities are distributed. They get access later, with less customization, and frequently without the deep coordination that financial or major tech players enjoy.

In a quantum migration context, that asymmetry would be even more dangerous. If high-resourced sectors migrate first and the OT-heavy backbone of national life lags by years, the entire national resilience picture suffers — even while certain industries look ready.

## VIII. What Infrastructure Leaders Should Be Doing Now

The right posture for the quantum migration era is not panic. It is early, disciplined execution. That looks like:

- Building a cryptographic inventory across IT, OT, vendors, and embedded devices;

- Establishing cryptographic agility so systems can swap algorithms without ripping out infrastructure;
- Engaging vendors early about PQC roadmaps and contract obligations;
- Prioritizing identity, signing, and authentication systems that defend system trust;
- Hardening OT environments so they are not a parallel cryptographic blind spot;
- Aligning with federal guidance and standards as they emerge; and,
- Treating PQC migration as an executive-level program, not a backlogged IT task.

This is not an exotic security concept. It is the same disciplined approach the U.S. defense community uses for any long-cycle, mission-critical capability shift.

## IX. The Competitive Dimension

There is also a national-competitive dimension to this work. Quantum capability is becoming a strategic technology layer. Lawmakers from both parties have signed onto the NQIA Reauthorization with strong public support, citing the importance of U.S. leadership in quantum sciences for national security, economic growth, and global influence. The bill, with its embedded amendments, ties together quantum manufacturing, near-term applications, post-quantum cybersecurity, and expanded R&D infrastructure.

That signals something important: the U.S. is not preparing only for the defensive side of the quantum transition. It is also positioning itself for the offensive and economic sides. That means the policy environment will likely move faster than many leaders expect. Migration timelines that look comfortable today may become tight quickly, particularly for sectors that touch national security indirectly through dependencies on telecom, finance, energy, or defense.

## X. Bottom Line

The quantum clock is already running because the threat is asymmetric, patient, and pre-positioned. Adversaries can harvest encrypted data today and decrypt it later, which means the strategic damage starts long before any public quantum milestone arrives.

The Senate's advancement of the National Quantum Initiative Reauthorization, the embedded National Quantum Cybersecurity Migration Strategy, the broader Trump administration cyber strategy, the active Iran-aligned OT intrusions, the strain on Cybersecurity and Infrastructure Security Agency , and the uneven distribution of frontier cyber tools to OT-heavy sectors all point in the same direction.

National resilience depends on cryptographic modernization, and the institutions that begin disciplined post-quantum migration now will be the institutions still standing when the rest of the country realizes how much catching up it has left to do

## ✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.

If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.

📩 Subscribe to Securing Our Future to gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance
3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.

This is built for professionals responsible for decisions that carry consequence—not commentary.

📅 Ready to operationalize these insights and move beyond theory?

👉 https://calendly.com/g1ve-technologies

Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

---

## 🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.

As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.

His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.

📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance