SCHOOL OF PUBLIC POLICY
CENTER FOR GOVERNANCE OF TECHNOLOGY AND SYSTEMS

May 2026

Securing the Transition to Post-Quantum Cryptography: Entropy, Scale, and Governance in an AI-Accelerated Threat Environment

Charles Harry, PhD

Center for the Governance of Technology and Systems (GoTech)

University of Maryland School of Public Policy

GoTech Policy Brief #02 | gotech.umd.edu

Executive Summary

The United States has entered a critical transition period in cryptographic security as advances in quantum computing an artificial intelligence (AI) converge to challenge the integrity of existing systems. Federal policy has already moved toward mandated action. National Security Memorandum-10 (NSM-10) directs that "the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant standards," while Office of Management and Budget (OMB) Memorandum M-23-02 requires agencies to inventory cryptographic systems and plan for migration to post-quantum cryptography (PQC).[1] The National Institute of Standards and Technology (NIST) reinforced this effort with the publication of core PQC standards in 2024.[2]

Yet the central challenge extends beyond replacing vulnerable algorithms. Many systems across federal agencies, contractors, and critical infrastructure rely on weak or uneven sources of entropy, which provide the randomness required to generate secure cryptographic keys. These weaknesses create immediate vulnerabilities that adversaries can exploit today using AI-enabled techniques, even before quantum computing becomes operational at scale. Beyond these immediate vulnerabilities, the implementation challenge is vast: the federal government obligates roughly $755–$773 billion annually across more than 100,000 contractors, spanning a highly heterogeneous industrial supply chain.[3]

---

[1] The White House, National Security Memorandum-10 (NSM-10) (2022); OMB, M-23-02 (2022).

[2] NIST, FIPS 203–205 (2024).

[3] GAO, Federal Contracting Overview. https://www.gao.gov/federal-contracting

The Challenge: An Evolving Threat Environment

PQC is often framed as a response to a future threat. In practice, policymakers face a dual-phase risk environment combining present vulnerabilities with future cryptanalytic capabilities. OMB explicitly warns that "cryptographic systems in use today will be vulnerable to quantum computers… [and] adversaries may harvest encrypted data now and decrypt it later."[4] This "harvest now, decrypt later" (HNDL) model reflects a widely recognized intelligence practice: encrypted communications can be collected and stored until advances in computation enable decryption.[5] Recent reporting suggests that large-scale state-sponsored cyber operations, including intrusions into telecommunications infrastructure[6], may support such long-term data collection strategies.[7] For example, Chinese attacks on U.S telecommunications infrastructure in the Salt Typhoon episode underscore this point with threat actors compromising a range of infrastructure including text, voice, and location data.

At the same time, current systems are already vulnerable due to weaknesses in how random numbers are generated.

---

[4] OMB, M-23-02.

[5] Mosca, Michele. "Cybersecurity in an era with quantum computers: Will we be ready?." IEEE Security & Privacy 16, no. 5 (2018): 38-41.

[6] Salt Typhoon is the designation tied to PRC linked intrusions into major telecommunications companies in the U.S. https://finance.yahoo.com/news/salt-typhoon-telecom-hacks-one-105842670.html.

[7] Dariia Mykhailenko, "Russian Cyber Hackers Use UK Routers to Redirect Internet Traffic and Steal Sensitive Data" , United 24 Media https://united24media.com/latest-news/russian-cyber-hackers-use-uk-routers-to-redirect-internet-traffic-and-steal-sensitive-data-17763

NIST emphasizes that “random numbers are critical to the security of cryptographic systems,” underscoring the centrali of entropy to cryptographic integrity.[8] When entropy is insufficient or poorly implemented, keys can become predictable, undermining even mathematically secure algorithms.

Artificial intelligence amplifies this risk. While AI does not directly break encryption, it enables adversaries to identify weak randomness, detect misconfigurations, and exploit implementation flaws at scale. AI-driven tools can automate vulnerability discovery across large systems, increasing the likelihood that entropy-related weaknesses will be identified and exploited. Anthropic’s Glasswing project is a clear example of this problem, where highly capable Large Language Models demonstrate the ability to identify vulnerabilities, some of which had remained buried for over 20 years.[9]

U.S. Policy Response: A Regulation-First, Algorithm-Centric Approach

The U.S. government has taken proactive steps through a coordinated set of mandates and standards. NSM-10 establishes strategic direction, while OMB M-23-02 requires agencies to act. Specifically, OMB states that “establish requirements for inventorying all currently deployed cryptographic systems, excluding National Security Systems” and prioritize high value systems.[10] NIST’s PQC standards define algorithms intended

[8] NIST, SP 800-90A.

[9] https://www.anthropic.com/glasswing

[10] OMB, M-23-02.

to be resistant to quantum cryptanalysis, providing a technic foundation for transition.[11] This approach reflects a regulatio first model designed to impose structure across a fragmente federal enterprise. It has been effective in establishing timelines, standardizing algorithms, and initiating system-wi inventory efforts.

However, the policy framework remains largely focused on algorithm substitution. It emphasizes what cryptographic standards to adopt, but gives comparatively less attention to how those systems are implemented. In particular, entropy generation, key management, and validation practices are not consistently treated as first-order policy concerns.

This potentially creates a gap between compliance and security. Agencies and vendors may adopt approved PQC algorithms while continuing to rely on weak or inconsistent entropy sources, resulting in systems that are formally compliant but operationally vulnerable.

Industry Response: Software, Hardware, and the Limits of Current Approaches

While U.S. policy has established standards and timelines, the pace and quality of the transition depend on how vendors integrate PQC into existing systems. Industry responses fall into two primary pathways: *software-based adaptation* and *hardware-based integration*, each with distinct tradeoffs.

Software-based approaches dominate in the near term. Cloud providers and platform vendors are incorporating PQC into

[11] NIST, FIPS 203–205.

protocols such as Transport Layer Security (TLS) and Virtual Private Networks (VPNs), often through hybrid models that combine classical and quantum-resistant algorithms. These approaches are attractive because they can be deployed rapi across existing infrastructure.

However, software-based solutions operate within existing system architectures. They improve the mathematical resilien of cryptographic schemes but do not fundamentally change how keys are generated. As NIST emphasizes full entropy is n required as long as the input "is accommodated by allowing length of the entropy input to be longer than the required entropy (expressed in bits), as long as the total entropy meets the requirements". [12] As a result, software-based PQC risks becoming a surface-level upgrade: stronger algorithms layered onto systems that may still produce predictable randomness enabling the ability to identify private keys through guessing the "random number" directly. AI-enabled tools further increase the likelihood that such weaknesses will be identified and exploited at scale. Recent advances in AI models including Anthropic' s Mythos[13] underscore the concerns tied to weak entropy.

A second pathway focuses on hardware. Vendors are developing hardware security modules, and dedicated entropy sources designed to support PQC. These approaches offer stronger assurance by embedding cryptographic functions and randomness generation directly into physical devices. Their limitation is scale.

---

[12] NIST, SP 800-90Ar1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

[13] https://www.anthropic.com/project/glasswing

Hardware upgrades are costly, slow, and difficult to deploy across heterogeneous environments. Many systems, particularly in critical infrastructure and embedded contexts- cannot be easily replaced. As a joint CISA, NSA, and NIST publication observes, "A successful post-quantum cryptograp migration will take time to plan and conduct."[14]

The result is a fragmented transition: software approaches enable speed but offer pathways for potential compromise d to weak entropy, while hardware approaches improve assurance but constrain scalability. Federal mandates are bui on the assumption of deployable solutions, but industry is advancing along uneven pathways.

Both approaches depend on high-quality entropy. Without addressing this underlying requirement, the transition to PQC risks reproducing existing vulnerabilities within a new cryptographic framework.

Scale and Constraints: Federal Networks, Industrial Base, and System Level Constraints

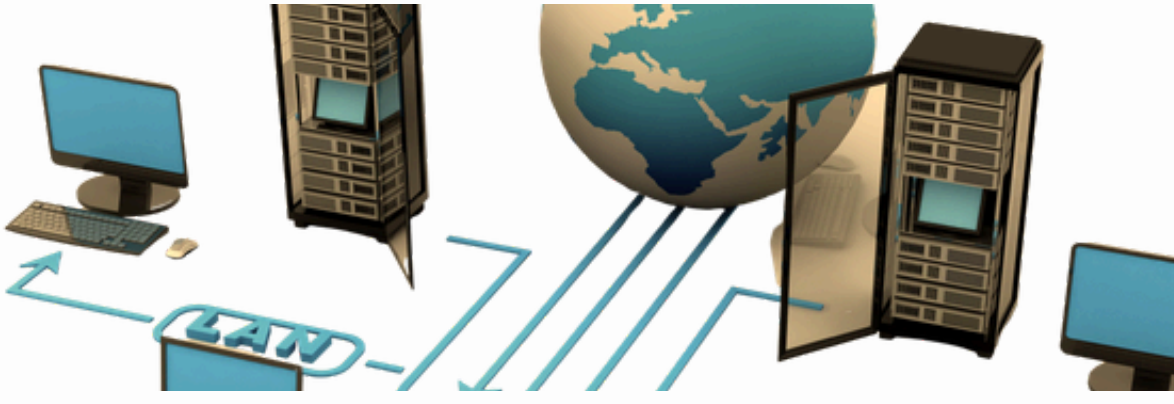
The complexity of PQC migration is driven by the scale of the federal contracting ecosystem. The U.S. government obligates approximately $755–$773 billion annually across more than 100,000 firms.[15] This ecosystem forms a deeply interconnected supply chain in which cryptographic functionality is embedded across software, hardware, and network infrastructure. Agencies often lack full visibility

[14] CISA,NSA "QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY", https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

[15] GAO, Federal Contracting Overview. https://www.gao.gov/federal-contracting

into these dependencies. Entropy-related vulnerabilities are particularly prevalent in this environment. Smaller vendors and embedded systems frequently rely on constrained hardware or legacy designs that do not support robust randomness. These weaknesses can propagate through supply chains, creating systemic risk that is difficult to detect and costly to remediate. PQC migration therefore becomes an industrial base coordination problem. Federal agencies cannot secure their systems without influencing vendor behavior across a highly distributed ecosystem.

The primary barrier to PQC migration is not algorithm availability, but the interaction of technical constraints, system complexity and cost structures. First, entropy remains a binding constraint. Systems with weak entropy cannot be secured through algorithm substitution alone. Second, system heterogeneity complicates implementation. Federal systems span legacy platforms, modern cloud environments, and embedded infrastructure, each with different upgrade cycles and technical constraints. Finally, these technical challenges translate directly into cost. OMB requires agencies to "prioritize systems based on risk," implicitly acknowledging resource constraints.[14] Costs include system discovery, validation, hardware upgrades, and contractor compliance. At scale, even marginal costs expand across a contractor base.



Policy Design for Scale: Coordinating a Complex System

Effective policy for post-quantum cryptography (PQC) cannot be designed as a traditional compliance exercise. The transition is occurring across a large-scale, heterogeneous, and interdependent system composed of federal agencies, contractors, vendors, and critical infrastructure operators. As such, policy must be designed to operate under conditions of complexity, uncertainty, and uneven capability.

From a systems perspective, PQC migration demonstrates the attributes of a complex adaptive system. Initially, the federal government must address the broad interdependencies present throughout supply chains. Vendors providing goods and services to the government also depend on additional suppliers, creating vulnerability to cascading effects. Furthermore, the government should consider the nonlinear escalation of costs linked to PQC migration, which can pose significant challenges for smaller firms. Ultimately, these financial pressures are likely to result in uneven adoption among participants, thereby introducing potential systemic risks that may not yet be recognized. Consequently, insufficiently coordinated interventions may inadvertently heighten risk rather than mitigate it.These dynamics mean that policy interventions must do more than mandate compliance; they must shape behavior across the system and align incentives at scale.

Recommendation #1: Elevate Entropy as a First-Order Policy Requirement

Randomness in key generation is not a feature that can be assumed, it is a system property that must be generated, maintained, and validated. Without sufficient entropy, even approved PQC algorithms can produce predictable keys, undermining security.
Policy should therefore:

- Establish minimum entropy standards for federal systems and contractors
- Require validation and testing of randomness sources, not just algorithm compliance
- Integrate entropy requirements into existing frameworks (e.g., NIST guidance, FISMA processes)

From a systems perspective, entropy functions as a shared dependency across all cryptographic operations. Failure to ensure its quality creates a common-mode vulnerability that can propagate across otherwise independent systems.

Recommendation #2: Use Procurement as a System-Level Lever

Federal procurement is the most powerful mechanism available for shaping behavior across the ecosystem. With over $755 billion in annual obligations, procurement functions as a market-making force, not merely an administrative process.

Rather than relying solely on agency-level compliance, polic should:

- Require vendors to disclose cryptographic implementations, including entropy sources
- Mandate PQC readiness and entropy assurance as conditions of contract eligibility
- Extend requirements to subcontractors and supply chai participants, not just prime contractors

This approach transforms procurement into a distributed enforcement mechanism, aligning incentives across a fragmented industrial base. Critically, procurement must address information asymmetry. Agencies often lack visibility into vendor systems, particularly at lower tiers of the supply chain. Requiring disclosure and certification reduces this asymmetry and enables more effective risk management.

↘ Recommendation #3: Implement Risk-Tiered Migration Across Systems

Not all systems require immediate or identical treatment. The current U.S directive to prioritize systems based on risk should be operationalized into a tiered migration framework.
A risk-tiered policy approach should:

- System criticality (national security, financial systems, infrastructure)
- Account for data longevity (how long confidentiality must be preserved),
- Exposure surface (public-facing vs. internal systems)

This allows policymakers to allocate resources efficiently, avoid overwhelming organizations with uniform mandates, and reduce systemic risk by securing the most critical syste first. From a systems perspective, this reflects targeted intervention at high-leverage nodes, a more effective strate than uniform, system-wide change.

Recommendation #4: Support Managed, Hybri and Phased Transitions

The transition to post-quantum cryptography will not occur as a discrete or synchronized shift. Instead, it is unfolding as a gradual and uneven process in which legacy and quantum-resistant systems must coexist for an extended period. In practice, this has led to the emergence of hybrid cryptographic models that combine classical and post-quantum algorithms as an interim solution.

While hybridization enables continuity and backward compatibility, it also introduces new layers of complexity. Systems must now support multiple cryptographic pathways simultaneously, increasing the attack surface and the likelihood of implementation errors. In many cases, these hybrid environments place additional demands on key generation and management, further straining already uneven sources of entropy.

These dynamics complicate what might otherwise appear to be a straightforward upgrade. The challenge is not just deploying new algorithms, but managing a transition across interdependent systems that are evolving at different speeds and under different constraints.

Policy should prioritize managed and phased transition strategies.

- Provide clear guidance on how hybrid systems should be implemented
- Establish timelines that reflect the realities of system lifecycles
- Ensure that organizations have mechanisms to monitor, evaluate, and adjust their implementations over time

Recommendation #5: Work with International Partners to Shape the Global Cryptographic Environment

The transition to post-quantum cryptography is not occurring within a single jurisdiction, but across a globally interconnected digital ecosystem. While the United States and its allies are converging on NIST-standardized algorithms, their approaches to implementation, timelines, and system assurance remain uneven. This divergence creates risks that cannot be mitigated through domestic policy alone.

Allied governments, including the United Kingdom, Canada, Germany, and Australia, have issued guidance on PQC migrati but differ in key areas such as deployment timelines, validation requirements, and the treatment of hybrid systems. In particul there is no consistent international approach to entropy assurance, randomness validation, or implementation verification, despite these being foundational to cryptographic security. As a result, systems that are nominally aligned at the algorithmic level may exhibit significantly different levels of rea world security.

To address this, policy should seek to:

- Leverage International Standards Bodies to Align Implementation Practices
- Promote International Standards for Entropy and Validation
- Coordinate Migration Timelines with Key Allies
- Use Trade and Security Partnerships to Reinforce Standards Adoption

PQC migration is a global coordination problem. Algorithmic convergence is necessary but insufficient; security outcomes depend on consistent implementation across jurisdictions. By shaping international standards and coordinating with partners, the United States can reduce fragmentation, align incentives, and help ensure that the transition to post-quantum cryptography delivers meaningful security improvements at the global level.

Conclusion

The transition to post-quantum cryptography is not simply a technical upgrade, but a governance challenge defined by scale, complexity, and system interdependence. PQC migration is inherently global. Allied governments have adopted similar standards but differ in implementation strategies and timelines. These differences create risks related to interoperability, supply chain fragmentation, and uneven security. Weak implementation in one jurisdiction can create vulnerabilities across interconnected systems.

Within the federal ecosystem, entropy-related vulnerabilities create immediate risk. AI-enabled techniques accelerate exploitation, while quantum computing increases long-term consequences. To succeed, policymakers must move beyond an algorithm-centric approach and adopt a systems-level strategy that emphasizes entropy assurance, supply chain coordination, and adaptive implementation. Without this shift, PQC migration risks reproducing the vulnerabilities it is intended to resolve.

Learn More About GoTech

@gotechumd

Contact us

Center for Governance of Technology and Systems
Thurgood Marshall Hall
7805 Regents Drive
College Park, MD 20742

gotech.umd.edu
gotech@umd.edu

GoTech Insights

Analysis and commentary on technology, governance, and human systems by experts at the Center for Governance of Technology and Systems (GoTech)

gotechinsights.com

Cyber Events Database

Timely, well-structured data on global cyber events to help decision-makers better understand the cyber threat landscape.

cybereventsdatabase.org