ICIT

Q Day Preparedness

White Paper & Recommendations

Authors: Brett Freedman, Hugo Holopainen, Cory Simpson, Javier Nater

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

TYCHON

Table of Contents

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s). To learn more, please visit www.icitech.org

Copyright 2026, The Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

I. Issue

The prospect of a Cryptographically Relevant Quantum Computer (CRQC),[1] capable of breaking the encryption underpinning the U.S. and global digital ecosystem ("Q-Day"), continues to advance.[2] Commensurately, the time agencies and critical infrastructure operators must prepare continues to narrow. The focus on migrating to Post-Quantum Cryptography (PQC) intensifies. This is not a distant, one-time technology refresh, but a near-term enterprise risk management challenge shaped by opaque ownership, limited visibility into cryptographic dependencies, constrained budgets, and both the persistent "harvest now, decrypt later" threat to sensitive data as well as the "Trust Now, Forge Later" threat pertaining to authentication. This white paper sets forth practical recommendations for how the Federal Civilian Executive Branch (FCEB) can begin closing those gaps now, while time to prioritize the most critical systems and data for transition remains.

II. Process

Beginning earlier this year, ICIT convened leading representatives from federal, industry, and policy stakeholders to assess U.S. preparedness for PQC migration and identify actionable priorities for the FCEB.

PQC migration is not a simple technical upgrade. To the contrary, it is a continuous enterprise risk management effort (think: vulnerability management) requiring governance clarity, prioritization discipline, data lifecycle awareness, and improved messaging.

Key themes of the discussions included:

- **A Shrinking Time Horizon -** Initially mandated as 2035 in both M-23-02 and NSM 10,[3] government is shifting to a 2030 planning horizon,[4] and industry momentum[5] appears to be coalescing around 2029.[6] Migration must be phased and prioritized. Providers require either legislative or policy mandates and/or a clear demand signal to focus their efforts on resiliency which the financial sector is already leading.

- **Execution Gaps -** Agencies lack consistent ownership, cryptographic visibility, and whole-of-government migration plans.

- **Resource Constraints -** In a resource constrained environment, large resource requirements will not automatically unlock new funding; as such, sequencing within existing budgets is critical.

- **Risk Reality -** "Harvest now, decrypt later" (HNDL) risks make long–lived sensitive data especially vulnerable.

- **Messaging Clenge -** PQC is often perceived as abstract or non–urgent; stakeholders must understand the short-term urgency as well as practical next steps.

III. Recommendations

1. Empower PQC Points of Contact (POCs) Across FCEB

Objective: Provide clear ownership and coordination.

Each agency should ensure, as mandated by NSM-10, that an agency-level PQC lead is designated and sufficiently empowered. The current list of agency PQC leads should be current and functional, with the POCs identified sufficiently empowered to execute their mandated functions.

These points of contact should be integrated with CIO, CISO, CFO, and enterprise architecture functions. Doing so will ensure that PQC migration is incorporated into the broader cybersecurity, modernization, financial, and systems planning efforts within the context of regular budget cycles rather than managed in isolation.
Cross-agency coordination and information sharing must be formalized across the FCEB. This will help agencies align priorities, share best practices, and advance migration efforts with greater consistency.

2. Prioritize Systems Through an Enterprise Architecture Lens

Objective: Effective inventory and execution.

Agencies should begin by identifying High Value Assets and other mission-critical systems that will require early attention in any PQC migration effort. As part of that process, the use of automated, off-the-shelf tools (Automated Cryptography and Discovery tools - ACDI) will be central to conducting the inventory at scale and improving visibility into complex enterprise environments.

Once complete, agencies should map where cryptography is embedded across their environments, including in legacy systems and commercially provided technologies that may be harder to assess or update.

In such efforts, government entities and critical infrastructure owners should work closely with industry partners to support assessment, planning, and implementation. In particular, critical legacy, OT, and ICS environments that may lack computing power or compatibility with PQC algorithms must undergo thorough assessments with industry partners for PQC risks.

The resulting visibility should then inform sequenced PQC transition plans, supported by Plans of Action and Milestones. Developing and executing those plans will require close coordination with vendors to support modernization efforts, particularly where agencies depend on commercial products or aging legacy systems that will be the most difficult to remediate. In practice, agencies should expect the burden of migration to be uneven, with a relatively small share of systems likely accounting for the majority of the cost and effort.

Wherever possible, those migration efforts should be aligned with broader modernization and technology refresh cycles to reduce disruption, make better use of existing resources, and position agencies to transition more efficiently.

3. Manage Data Lifespan & Long–Term Confidentiality Risk

Objective: Address “harvest now, decrypt later” exposure.

Agencies should identify the data and systems that require long-term confidentiality and are therefore most susceptible to future decryption risks. Once that data is identified, agencies will need clear tagging and classification practices to ensure it is properly distinguished according to sensitivity, access requirements, and expected lifespan. Those decisions will directly shape retention policies, archived data management, and broader determinations about which information must be protected for the longest period of time.

That assessment should inform a re-assessment of retention policies, encrypted archives, and other stored data practices that may otherwise extend exposure unnecessarily over time.

Agencies should also prioritize re-encryption strategies for critical datasets whose sensitivity will outlast currently deployed cryptographic protections.

Taken together, these steps help strengthen the data pillar within broader Zero Trust efforts and ensure that PQC planning is informed not only by system modernization needs, but also by the lifespan and sensitivity of the data those systems are meant to protect.

4. Tie PQC to Existing Funding Cycles (Without Losing Focus of Immediate & Necessary Steps)

Objective: Tie quantum cryptography implementation to tech capital expenditure cycles to secure funding (both AI & quantum share the same funding timelines and 2029-2030 planning horizon).

Agencies should align PQC migration with existing technology capital expenditure cycles rather than assume that new, dedicated funding will materialize. In practice, that means integrating PQC upgrades into existing IT modernization programs and treating PQC as a component of broader Zero Trust architecture, especially because most agencies are unlikely to receive additional appropriations specifically for PQC migration.

Agencies should also look to established funding vehicles, including legislative (such as NDAA) and relevant state, local, tribal, and territorial funding avenues, to support planning and implementation where possible.

At the same time, AI can serve as a useful messaging bridge to raise leadership awareness, given that AI and quantum are often discussed on similar investment and planning timelines.

However, treating PQC as a secondary add-on to AI infrastructure after the fact should be avoided as remediation would be more costly and complex.

Conflating AI innovation goals with the distinct fundamentals of PQC migration should also be avoided. However, where appropriate, agencies should explore AI-enabled tools to support discovery, asset mapping, and prioritization as part of a broader, disciplined migration strategy.

5. Improve Messaging & Education

Objective: Create urgency and basic awareness without triggering resistance.

Agencies should communicate PQC in practical, operational terms rather than as an abstract scientific or technical issue. Messaging should clarify that enterprise-wide awareness is more important than highly specialized technical expertise, and that personnel do not, for example, need a PhD in physics to understand PQC and begin taking meaningful action.

Sequenced, achievable steps that can be pursued within existing budgets, while tailoring communications for relevant Congressional vehicles and committees, including quantum-related legislative efforts, should be emphasized.

Just as important, messaging should reflect that PQC awareness remains uneven across sectors: the financial sector is generally farther ahead, while many critical infrastructure owners and operators may not yet be tracking these issues closely.

For that reason, outreach and education efforts should be designed to meet audiences where they are, with concrete guidance that makes clear this is a current risk requiring action now rather than a distant future problem.

IV. Conclusion

As highlighted in the 2026 Cyber Strategy for America,[7] the transition to Post-Quantum Cryptography must begin immediately. Objectively, the PQC transition is a long migration process. It cannot be completed overnight or within a fiscal year. The federal government has provided the foundational guidance in the form of executive branch edits and accompanying policies and procedures. Urgent action by Congress and Executive Branch agencies is needed to allocate the necessary resources and strengthen government preparedness and to get the broader message out to critical infrastructure owners and operators. The recommendations contained in this report are intended to help provide a framework of how to approach their PQC transition and set the nation on a path to PQC resilience.

V. Bibliography

References

1. Marin Ivezic, “Cryptographically Relevant Quantum Computers (CRQCs),” PostQuantum.com, January 10, 2023, https://postquantum.com/post-quantum/crqc/.
2. Heather Adkins and Sophie Schmieg, “Quantum Frontiers May Be Closer Than They Appear,” The Keyword, March 25, 2026, https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/.
3. Executive Office of the President, Office of Management and Budget, Migrating to Post-Quantum Cryptography, Memorandum M-23-02 (Washington, DC: Office of Management and Budget, November 18, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.
4. Dylan Presman, “NSM-10 and the Transition to Post-Quantum Cryptography,” slide presentation, Fifth PQC Standardization Conference, National Institute of Standards and Technology, April 10, 2024, https://csrc.nist.gov/csrc/media/Presentations/2024/u-s-government-s-transition-to-pqc/images-media/presman-govt-transition-pqc2024.pdf.
5. Heather Adkins and Sophie Schmieg, “Quantum Frontiers May Be Closer Than They Appear,” The Keyword, March 25, 2026, https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/.
6. Bas Westerbaan, “Cloudflare Targets 2029 for Full Post-Quantum Security,” The Cloudflare Blog, April 7, 2026, https://blog.cloudflare.com/post-quantum-roadmap/.
7. The White House, President Trump’s Cyber Strategy for America (Washington, DC: The White House, March 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

VI. Authors & Taskforce

Brett Freedman

Senior Director, Emerging Technology, Institute for Critical Infrastructure Technology (ICIT).

Brett Freedman has nearly two decades of experience at the highest levels of government. A Partner and Head of Government Affairs at Gray Space Strategies, a strategic advisory firm, Brett's public service career includes serving as a Legislative Assistant for a Congressman and as a Presidential Management Fellow in the Department of Homeland Security. Brett was an Attorney at the National Security Agency and in the National Counterterrorism Center in the Office of the Director of National Intelligence.

In 2013, Brett served as the Counsel to the President's Review Group on Intelligence and Communications Technologies which examined the disclosures of classified information by Edward Snowden. He then served as Counsel to the Senate Select Committee on Intelligence, including as General Counsel for then-Chairman Mark R. Warner (D-VA). Most recently, Brett was Chief of Staff for Assistant Attorney General Matthew G. Olsen of the National Security Division at the Department of Justice, helping oversee the daily operations of several hundred attorneys in foreign investment, counterterrorism, counterespionage, and cybersecurity.

Brett holds a Juris Doctorate, a Master of Law and Diplomacy, and a Bachelor of Arts in International Affairs. He is also an Adjunct Professor at Georgetown University in cybersecurity.

Hugo Holopainen

Senior Associate, Research & Content Development Lead, Institute for Critical Infrastructure Technology (ICIT)

Hugo Holopainen leads research and content development at ICIT and Gray Space Strategies, bringing technical depth and disciplined analysis to the organization's engagements. Hugo researches the intersections of cybersecurity, aerospace, critical infrastructure, emerging technology, and defense.

He brings experience across security and international environments, with a background spanning military service, diplomatic work, and emerging technology. His work focuses on understanding complex systems, analyzing technical developments, and translating that understanding into immediate decisions and longer-term positioning and program direction. His work bridges defense, cyber, and emerging technology to inform strategy at the nexus of security and innovation.

Cory Simpson

Chief Executive Officer, Institute for Critical Infrastructure Technology (ICIT).

Cory Simpson has over twenty years of experience in government, the military, and the private sector, specializing in national security, cybersecurity, business, law, and strategy. He served in the U.S. Army Judge Advocate General's Corps from 2004 to 2016 and continues as a legal advisor to U.S. Army Cyber Command. His military career includes roles as general counsel, prosecutor, and national security law advisor, with multiple combat tours and extensive trial experience. Cory is the CEO of Gray Space Strategies, a strategic advisory firm, and the Institute for Critical Infrastructure Technology (ICIT). He also serves as a senior advisor to CSC 2.0, continuing the work of the U.S. Cyberspace Solarium Commission, and is on the Board of Directors for the Cyber Guild.

Cory holds a Master of Laws in Military Law, a Juris Doctorate, and a BA in accounting with a minor in philosophy. He is globally recognized for creating effective solutions to complex challenges.

Javier Nater

Director of Operations, Institute for Critical Infrastructure Technology (ICIT)

Javier Nater is the Director of Operations at Gray Space Strategies and ICIT, ensuring engagements are planned, coordinated, and executed with discipline.

Javier sits at the center of the organizations' operations, translating strategy into execution and ensuring that the work led by the leadership is executed consistently, precisely, and with accountability.

He brings a strong academic foundation and a practical approach to problem-solving, supporting work across cybersecurity, national security, and emerging technology. His focus is on building and managing the systems, processes, and coordination required to operate effectively in complex environments.

At both organizations, Javier works closely with leadership to manage priorities, align efforts, and maintain the pace and discipline needed to deliver. His role enables the organizations to move quickly, stay organized, and sustain a high standard of execution across engagements.

This report was prepared in collaboration with agencies and organizations including:

Cybersecurity and Infrastructure Security Agency

National Security Agency

Office of Science and Technology Policy

Office of the National Cyber Director

Office of Management and Budget

United States Department of the Army

United States Department of the Navy

National Institute of Standards and Technology

Thanks to our sponsors for making this work possible:

TYCHON

ICIT

www.icitech.org

Copyright 2026, The Institute for Critical Infrastructure Technology (ICIT)