Statement for the Record

From Dr. Yaakov Weinstein and Dr. Moses Liskov, The MITRE Corporation

For the House Committee on Oversight and Accountability

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Hearing, "Preparing for the Quantum Age: When Cryptography Breaks"

June 25, 2025

Chairwoman Mace, Ranking Member Brown, members of the committee,

Thank you for the opportunity to provide a statement for the record on matters relating to post-quantum cryptography and the advent of a quantum computer.

We are providing this statement today on behalf of the MITRE Corporation. MITRE is a non-profit, non-partisan research institution that operates Federally Funded Research and Development Centers (FFRDCs) on behalf of the U.S. Government. Among other technical disciplines, our team of quantum scientists and technical experts provide deep expertise across the executive branch, including in support of organizations like the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and the Department of Defense.

The speed and processing power of quantum computers will revolutionize research in cybersecurity, defense, finance, manufacturing, and health. MITRE has been working to support national priorities to develop quantum computing benchmarks and metrics, design and construct quantum computing hardware, and develop quantum algorithms, including those based on AI and machine learning, to improve optimization, logistics, and synthetic data generation. MITRE also has a concentrated emphasis on other quantum technologies including sensing, communications, and materials.

The revolutionary potential of quantum computers first became apparent 30 years ago with the discovery that a quantum computer could break the mathematical basis protecting the vast majority of encryptions given current methods. Should these algorithms be compromised, huge amounts of classified and other encrypted data would immediately become vulnerable.

Adversary nations are harvesting encrypted data from U.S. communications in hopes of compromising the encryption once a quantum computer becomes available. Given that some classified data must remain so for decades, perhaps beyond the time when quantum computers become available, it is necessary to address the quantum computer threat as

soon as possible to ensure the protection of classified data in the event this transformative technology is realized.

In addition to accessing encrypted data, quantum computing could also compromise digital signatures – an essential component to securing computer systems. This could lead to grave impacts: digital signatures are an essential part of many highly important mechanisms, including for instance securing financial payment systems, command and control of weapon systems, energy and transportation systems, not to mention general computer security of all kinds.

Industry and governments throughout the world are racing to have the first cryptographically relevant quantum computer. The strongest efforts outside of the United States are occurring in China and the European Union. China specifically has shown marked capabilities in some cases rivalling United States industry efforts. MITRE has discussed predictions on the pace of quantum computer maturity in a number of publications we have authored[i]. In this statement, we discuss how to counter the quantum computing threat and what is being done about it.

Concern for future quantum computers that can decode already harvested encrypted data has motivated National Institute of Standards and Technology (NIST)[ii] and other federal agency efforts to create and mature new cryptographic methods known as post-quantum cryptography (PQC) – cryptographic algorithms and protocols designed to be secure against attacks from quantum computers – a conventional defense against a quantum threat. In addition, the need for protection against the quantum computing threat has been codified on the federal level by:

- NSA's Cybersecurity Advisory Commercial National Security Algorithm (CNSA) Suite 2.0,[iii] which mandates timelines by which national security systems must migrate to PQC
- The Quantum Computing Cybersecurity Preparedness Act,[iv] which requires each agency to maintain an inventory of information technology vulnerable to the threat of a quantum computer, and the Office of Management and Budget to issue guidance requiring each agency to develop a plan to migrate to PQC
- National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,[v] an executive order issued in 2022 mandating that the US federal government mitigate "as much as is feasible" of the quantum risk to cryptography by 2035, and also mandating requirements for gathering and submitting inventories of affected systems and budget estimates to OMB.

Thanks to these untiring efforts of NIST and other federal agencies, we have mature and stable PQC algorithms that can secure the nation's information systems against the threat of a quantum computer.

These algorithms are based on mathematical problems believed, through wide and open research, not to be solvable efficiently using either conventional or quantum computers. As of June 2025, NIST has finalized standards for three PQC algorithms, including the ones that NSA has approved for use in national security systems. Various implementations of these algorithms exist, including in some formally validated cryptographic modules. However, broader availability of PQC in systems is still yet to come, and it is vital that federal and state agencies as well as industries of national importance prioritize migration to PQC for their most critical systems.

The MITRE Corporation is working in three primary ways to assist with the transition to PQC:

1. MITRE directly supports a variety of government sponsors to respond to the quantum threat: planning for a migration, testing and evaluating PQC algorithms and protocols, and providing expertise to help them overcome technical challenges and meet federal mandates for inventory and budget reporting. Legislative and Administrative requirements to make specific plans and estimate budgets for PQC migration have encouraged federal agencies to engage with the technology vendor community, leveraging the combined buying power of the federal government to encourage creation of a market for PQC adoption in commercial products.
2. MITRE was a founding member of the Post-Quantum Cryptography Coalition (PQCC),[vi] an industry collaboration which brings together technologists, researchers, and expert practitioners to drive progress towards broader understanding and public adoption of PQC. MITRE collaborates with the other members of the PQCC to produce assessments of cryptographic standards and artifacts for organizations to plan their migration to PQC, among other collaborative endeavors to advance the field.
3. The MITRE ATT&CK framework is a freely accessible knowledge base of adversary tactics and techniques which has revolutionized the way the world handles and prepares for cybersecurity attacks. In the lead up to a quantum threat, MITRE is building on this successful model to construct a parallel ATT&Q framework to prepare for the threats enabled by quantum computers and other emerging quantum technologies. Though not yet public, MITRE is currently working with the government to ensure the technical viability and usability of this framework.

While the advent of mature quantum computers carries significant benefits, these systems also pose a grave threat to United States security and economic infrastructure. The United States has set up the basic elements for defense against the threat, protocols that can withstand a quantum computer attack, federal direction to put these in place, and standards that apply to the private sector. However, it is not sufficient to only have these

tools, it is a national imperative, now, to ensure their adoption across the public and private sectors.

---

[i] Quantum Computing: Quantifying the Current State of the Art to Assess Cybersecurity Threats

[ii] What Is Post-Quantum Cryptography? | NIST

[iii] National Security Agency, "Announcing the Commercial National Security Algorithm Suite", September 2022. Available: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[iv] H.R. 7535 – 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act." Available: https://www.congress.gov/bill/117th-congress/house-bill/7535/text

[v] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" (NSM 10), May 4, 2022. Available: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[vi] Post-Quantum Cryptography Coalition