House Homeland Security: **“The Quantum, AI, and Cloud Landscape: Examining Opportunities, Vulnerabilities, and the Future of Cybersecurity”**

December 17, 2025

Good morning, Chairman Garbarino, Ranking Member Thompson, Chairman Ogles, Chairman Brecheen and members of the committee. Thank you very much for the opportunity to testify today.

My name is Eddy Zervigon, and I am the CEO of Quantum XChange. We were founded in 2018, two years after NIST was tasked with evaluating the algorithms to take us into the quantum age. Quantum XChange is a cybersecurity company that interoperates with the major network infrastructure vendors to enable the encryption that protects data today and into the post-quantum future with hardware and software solutions developed entirely in the United States.

While quantum computing and AI promise new breakthrough capabilities, they also introduce significant risks to our national and economic security that must be urgently addressed. AI can enable faster, more dangerous cyberattacks and quantum computers can break current encryption standards, exposing sensitive data. These capabilities will be weaponized by our adversaries, creating a very dangerous imbalance in our cyber defenses.

For more than 50 years, encryption has safeguarded our data from theft and misuse. We've had the luxury of a "set it and forget it" mindset, trusting its strength by default. That era is now ending with quantum computing.

Think about it like this:

Imagine all digital communications from government agencies sent over the past ten years being readable by our adversaries. This is a real threat to the US today; rogue nation states and state-sponsored terrorist groups are collecting encrypted data NOW to decrypt later with a quantum computer.

Further, now imagine our adversaries reading sensitive government data in real time, and altering it without anyone knowing. This could be tomorrow's reality.

Public and private sector work on quantum-resilient solutions is ongoing. Technologies, like post-quantum cryptography (PQC) *or quantum-safe encryption algorithms*, are part of the solution but not the complete answer. Despite our best efforts, post-quantum cryptography may still be vulnerable to quantum-enabled attacks.

All of which raises this fundamental question and challenge:

> *What happens when an algorithm breaks (because it is a when, not if)? Every agency CIO, enterprise CISO, security vendor, and network gear manufacturer must be able to answer that question.*

In our view, what’s needed to ensure data security and confidentiality in the quantum age is an architectural approach, not just a new algorithm.

This architectural approach enables agencies to focus on securing the network that data travels on to strengthen the existing infrastructure against quantum attacks, while minimizing disruption to existing operations. This is how our government agencies need to be protected. When you have valuables in your house, the first step isn’t buying a new jewelry box with biometric access controls, it's locking your front and back doors, so the house is secure and harder to get in. Once your home is secure, then you can figure out what specific rooms need further locks or security measures to protect your valuables and sensitive documents.

Federal agencies handling sensitive data need to act now and follow the lead set by Customs and Border Protection. Our work with CBP to incorporate PQCs across their network infrastructure in 2026 has shown that you **can** begin to secure your networks *today* with quantum-resistant technologies in a FIPS validated way, without having to rip and replace your entire infrastructure. I cannot stress enough that timing here is critical.

Agencies that fail to prepare today risk leaving their data vulnerable. Every day that we are not quantum-resistant is another day that data is harvested, to be decrypted later. It is important to note, that we at Quantum XChange are not the only ones advocating for action today. The Quantum Industry Coalition, which we are a part of and includes Amazon Web Services, Google, IBM, Microsoft, Accenture, and others believes “that *agencies handling sensitive government data should already be actively preparing for the transition and should begin migrating high-risk systems to FIPS/NIST validated PQC where possible.*

Having the opportunity to meet with several of your offices, I was often asked “What can Congress do?” Through this committee’s leadership, and building off the work previously done, Congress can accelerate the timelines for PQC compliance, allocate the budget to allow the migration process to begin, and work with leaders within the Administration to encourage adoption, as the technology is readily available and deployable today. America’s defenses cannot stop at our physical borders. Through your leadership and efforts, and in partnership with private sector partners like us, we can and will secure America’s digital borders too.

In closing, I want to thank you all again for the opportunity to offer some thoughts today and look forward to your questions.

Eddy Zervigon

QIC Quantum
Industry
Coalition

Quantum Industry Coalition Position on Post-Quantum Cryptography

October 23, 2025

The National Institute of Standards and Technology (NIST) has approved the first set of post-quantum cryptographic (PQC) algorithms, in what promises to be an iterative process moving forward. NIST has been leading the migration charge for close to a decade, evaluating and approving the algorithms and delivery architectures that will protect our data networks into the post-quantum era.

The Federal government has set timelines for the adoption of these post-quantum algorithms through legislation and executive orders. Government agencies should already be preparing for PQC transition through education, cryptographic inventory, risk assessments, transition strategies, and pilots. At the same time, the ecosystem of innovative start-ups and established players surrounding the delivery of these algorithms has progressed to a point where transition is possible in some high-risk areas, such as securing the network layer.

It is our position that agencies handling sensitive government data should already be actively preparing for the transition and should begin migrating high-risk systems to FIPS/NIST validated PQC where possible.

Quantum Industry Coalition Members Include:

Accenture

D-Wave

Entanglement Institute

IonQ

Quantinuum

Rigetti Computing

Xanadu

Amazon Web Services

Cold Quanta

Diraq

Google

MesaQuantum

Quantum Corridor

SandboxAQ

Anametric

EeroQ

IBM

Microsoft

Quantum Machines

SEEQC

Atom Computing

enQase

Infleqtion

Qolab

Quantum XChange

Strangeworks