



February 23, 2026

Ohio House of Representatives  
Technology and Innovation Committee  
State Capitol  
1 Capitol Square Columbus, OH 43215

**Re: Support for Ohio House Bill 650 – Advancing Cybersecurity and Future-Ready Cryptographic Protection**

Dear Chair Claggett, Vice-Chair Workman, and Distinguished Members of the Committee:

I write today on behalf of Palo Alto Networks to express our strong support of Ohio House Bill 650, an essential legislative initiative that acknowledges the rapidly evolving cyber threat landscape facing both public and private infrastructure. As the Committee evaluates this measure and the establishment of the Frontier Technologies and Quantum Computing Commission, I urge you to address the immediate threats facing Ohio’s critical systems, as well as the emerging threats posed by near-term advances in quantum computing.

**Scope of the Cybersecurity Challenge: Global, State, and Local Vulnerabilities**

Across the globe, critical infrastructure—from energy grids to transportation networks, from health systems to financial services—relies on digital connectivity and cryptographic protections to ensure confidentiality, integrity, and availability. These protections are foundational: they secure communications (e.g., TLS/HTTPS and VPNs), authenticate identities, and protect sensitive data in transit and at rest. Yet, these very mechanisms are under unprecedented threat. Classical asymmetric encryption—upon which most digital trust models are based—is vulnerable not only to conventional cyber adversaries exploiting misconfigurations and weak identity controls, but also to future *cryptographically relevant quantum computing* (CRQC) advances that could, in potentially short order, render today’s encryption schemes ineffective.

A hallmark of this emerging threat is the risk of “harvest now, decrypt later” attacks, where adversaries capture encrypted data today with the intent of decrypting it once quantum capabilities matures. This means that data with enduring value—historical health records, intellectual property, long-term contracts, legal documents—could be irreversibly compromised unless systems migrate to quantum-resistant standards now.

For states like Ohio, with robust manufacturing, healthcare, financial services, and academic sectors, the implications of delayed preparation are profound. Legacy systems, Internet of Things (IoT) ecosystems, and operational technology (OT) networks often lack modern cryptographic agility, increasing exposure across the public and private sectors. To ensure we don’t replace legacy IT/OT with soon-to-be legacy IT/OT, it’s critical that those necessary investments account for cryptographic resilience to provide more durable security.

## Opportunities for Ohio: A Cybersecurity and Innovation Advantage

House Bill 650 presents Ohio with a strategic opportunity to lead rather than react. By encouraging the adoption of post-quantum cryptographic (PQC) readiness measures, Ohio can:

1. **Enhance State Infrastructure Resilience** – Promote risk assessments and cryptographic inventories for state agencies and critical service operators. Most enterprises today are constrained by cryptographic debt – years of accumulated, undocumented and deprecated encryption protocols buried deep within legacy applications, third-party software libraries and unmanaged IoT devices. This creates a vast and largely invisible attack surface. The visibility derived from identifying all cryptography across endpoints is foundational for prioritizing upgrades and reducing exposure to both classical and quantum threats.
2. **Drive Workforce and Economic Development** – Support training programs focused on quantum-ready cybersecurity practices. Equipping Ohio’s workforce with skills in cryptography, network defense, and risk management elevates the state’s competitiveness and attracts business investment in secure digital transformation.
3. **Accelerate Public-Private Collaboration** – Enable frameworks where state agencies, private sector partners, and academic institutions share threat intelligence, best practices, and innovation related to quantum-resilient solutions. Establishing Ohio as a hub for quantum-cybersecurity research reinforces the state’s reputation for forward-looking policy.
4. **Protect Residents and Consumers** – As sectors such as banking, healthcare, and utilities adopt PQC and related safeguards, Ohio citizens benefit from increased protection against identity theft, fraud, and data breaches.

The technology community is already responding. Leading cybersecurity solutions now include integrated support for standardized PQC algorithms, quantum-safe VPNs, hybrid post-quantum cryptographic support, and tooling around automated cryptographic inventories. These capabilities help organizations transition incrementally and strategically to quantum resilience without disrupting operations.

## The Necessity for Thoughtful, Urgent Legislative Engagement

The accelerated pace of digital transformation—coupled with the exponential potential of quantum computing—demands that legislators act with both urgency and deliberation. This is not a distant concern: industry projections suggest that cryptographically relevant quantum capabilities could arrive within the next five years, compressing timelines for preparedness. Effective policy must therefore balance risk reduction with innovation support, ensuring Ohio’s institutions are capable of modern cryptographic evolution and threat response.

Moreover, cybersecurity is not merely a technological issue—it is a matter of economic security, personal privacy, and public safety. Legislation like HB 650 signals to businesses and residents alike that Ohio is prioritizing trust in digital services, continuity of essential functions, and resilience against both existing and emergent threats.

Ohio House Bill 650 represents a meaningful, forward-looking response to an evolving and expanding threat landscape. The proposed Frontier Technologies and Quantum Computing Commission encourages governmental agencies, NGOs, and private sector partners to engage on quantum-era cybersecurity challenges today and will help Ohio position itself at the forefront of risk management, economic opportunity, and digital trust.

I appreciate the Committee's consideration and I am available to provide any additional support or expertise as this important legislation progresses.

Respectfully,

A handwritten signature in black ink, appearing to read 'Thomas MacLellan', is positioned above the typed name. The signature is fluid and cursive.

Thomas MacLellan  
Director, Government Affairs  
Palo Alto Networks