



PREPARE TODAY FOR TOMORROW'S QUANTUM THREATS

Protect your critical data with a practical roadmap to post-quantum cryptography.

Sensitive data encrypted today could become readable tomorrow. As quantum computing advances, federal agencies must begin preparing now to protect mission-critical systems, safeguard sensitive information, and respond to the federal mandate to transition vulnerable cryptographic systems to quantum-resistant cryptography. Organizations need more than new algorithms - they need a strategy for managing cryptographic risk across their entire technology environment.

Iron Bow brings direct experience deploying PQC-safe network architectures for federal customers, combined with deep expertise across classified networking, PKI, identity, Zero Trust, and cybersecurity modernization. We help customers assess their current posture, prioritize critical systems, and build a phased roadmap aligned with evolving federal guidance and mission priorities.



**White House
Mandated
by 2035**

The Quantum Computing Challenge

Public-key cryptography secures nearly every digital interaction, from sensitive customer information to government communications. Quantum computing will eventually render many of today's public-key cryptographic algorithms vulnerable, creating significant long-term cybersecurity risk.

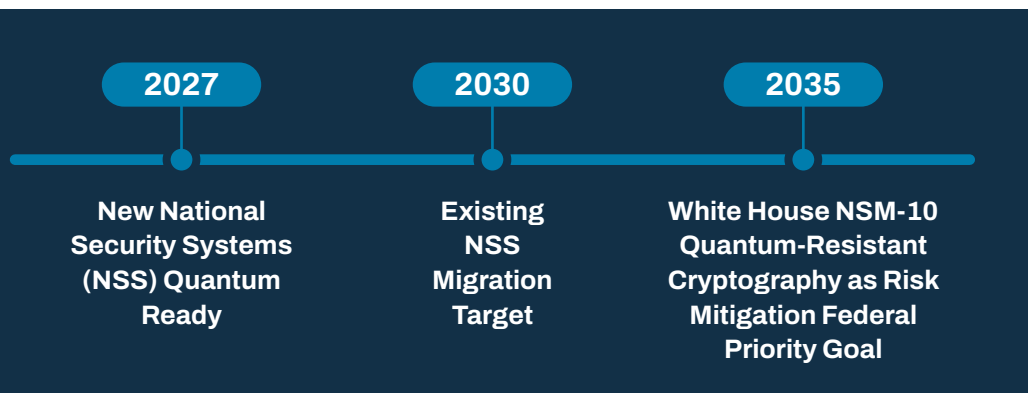
Adversaries are already collecting encrypted data with the expectation that it can be decrypted once quantum capabilities mature - a strategy known as **Harvest Now, Decrypt Later**.

Organizations that rely on long-lived sensitive data should begin planning their transition to post-quantum cryptography today.

HARVEST NOW

DECRYPT LATER

Key Federal Timelines



Where Quantum Risk Matters to Federal Agencies



Migration Path

The migration to quantum-safe cryptography is a multi-year journey, not a last-minute upgrade. Iron Bow's holistic migration path supports the entire tech stack and IT environment.

- Assess**
Inventory cryptographic assets and identify long-lived sensitive data
- Prioritize**
Evaluate mission risk and establish migration priorities
- Design**
Develop crypto-agile architectures using approved PQC algorithms
- Validate**
Test interoperability, performance, and vendor readiness
- Migrate**
Deploy quantum-safe capabilities while continuously monitoring evolving standards

Why Iron Bow

- ✓ **Direct experience** deploying PQC-safe network architectures
- ✓ **Deep expertise across** Zero Trust, PKI, identity, and cybersecurity modernization
- ✓ **Commercial Solutions** for Classified (CSfC) Trusted Integrator
- ✓ **End-to-end** services spanning assessment, planning, implementation, and operational support

**Learn
more!**

Begin building your quantum-ready future.
Email pqc@ironbow.com to schedule a Quantum Readiness Assessment.

ironbow.com/pqc

Iron Bow Technologies
2121 Cooperative Way, Suite 500
Herndon, VA 20171
www.ironbow.com

© Iron Bow Technologies. All rights reserved.