NSM-10 and the Transition to Quantum Resistant Cryptography

October 2023

Dylan Presman

Agenda

- Background: Opportunities and Risks
- Administration's Position: Policy Roadmap
- Where Are We?

Background: Opportunities and Risks

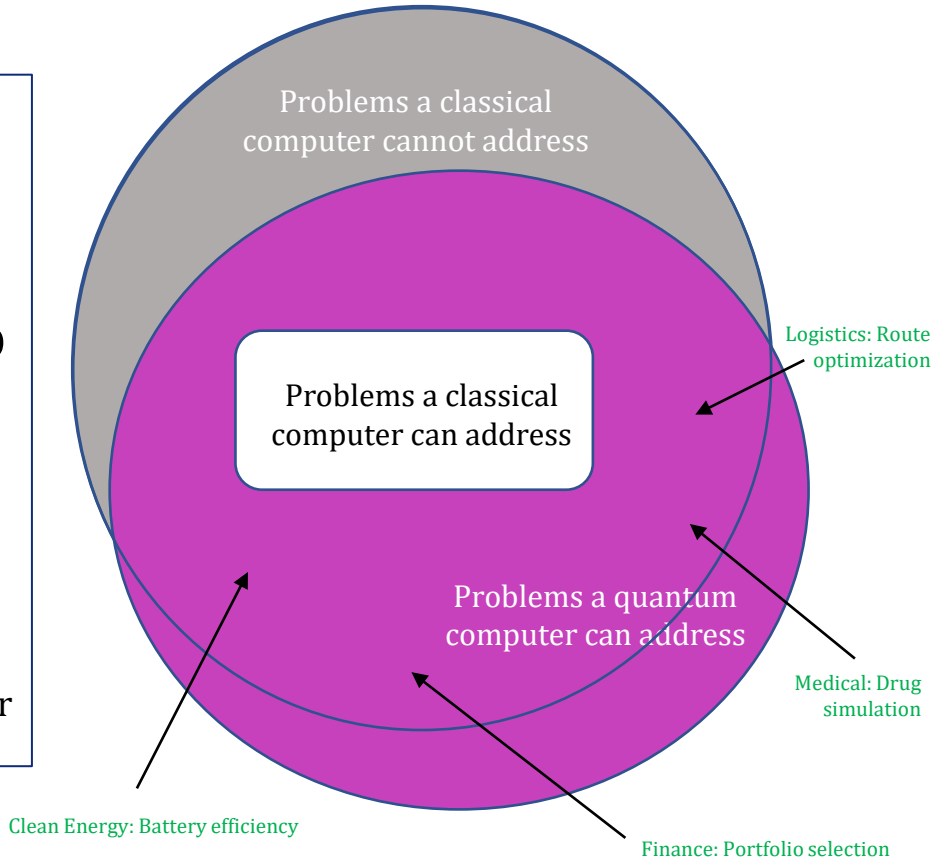
Quantum computers: Unimagined Opportunities

- Quantum as "spooky science": Superposition, Entanglement, and Peter Shor

Simulating Chemical Reactions

We would need 10^{48} bits to represent the energy reactions of a caffeine molecule on a classical computer, but 160 qbits

-Gabe Chang, IBM Quantum Ambassador

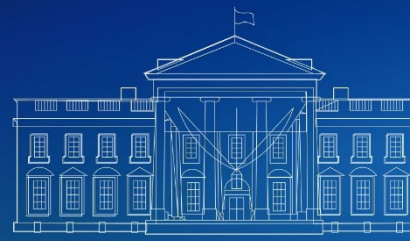


Shor's Algorithm

"The RSA-2048 Challenge Problem would take 1 billion years with a classical computer. A quantum computer could do it in 100 seconds"

-Dr. Krysta Svore, Microsoft Research

Background: Opportunities and Risks



BLUF: Quantum computers will render today's cryptography useless

All Modern PKI Encryption Impacted	Cybersecurity Transition Timelines are Long	Long Term Data Privacy Shelf-life Reduced
Encryption based on RSA, DH, ECC can be broken using Shor's algorithm on a sufficiently mature quantum computer	Transitioning cryptographic technology is difficult and will take decades to reach mass adoption	Data secured with classic encryption requiring many years of privacy will have its shelf-life significantly reduced or eliminated

Key Considerations

Harvest Now Decrypt Later

Data with a long confidentiality requirement needs to be protected now.

Legacy IT

Some systems cannot migrate to PQC and will need to be replaced

Prioritization

Multi-Factor Authentication, classical encryption are the best defenses

Budgeting

Budgets look at what can be done in the next year

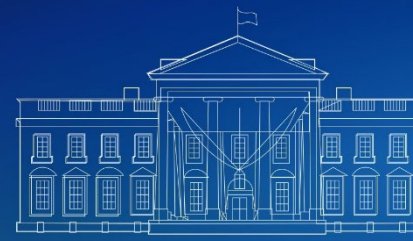
Cryptographic Agility

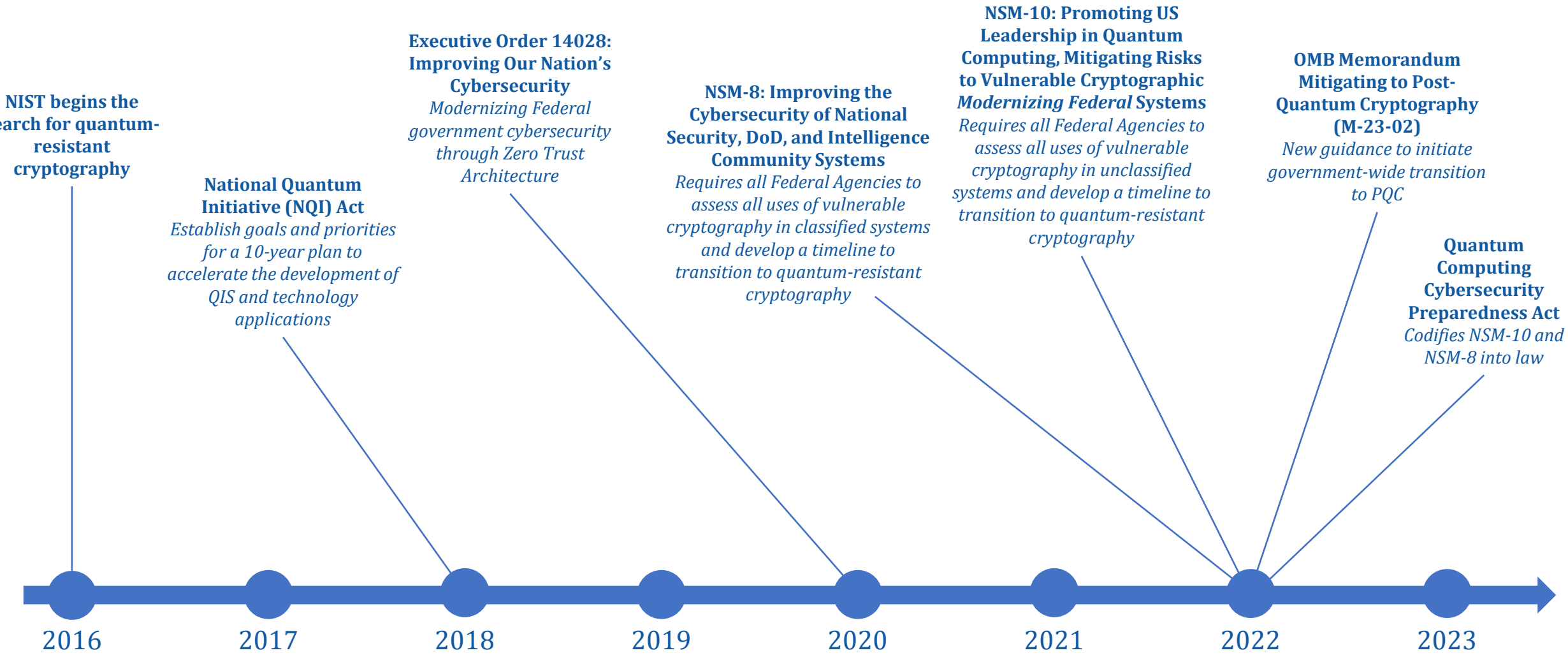
This won't be our last cryptographic modernization

Industry Adoption

Government and Industry will drive each other's PQC migration

Quantum Policy Timeline





Where Are We?

- **May 4, 2023:** Federal Agencies submitted prioritized inventory of cryptographic systems through CISA's CyberScope reporting system
- **June 3, 2023:** Federal Agencies submitted initial cost estimates
- **August 2023:** NIST released draft standards for quantum- resistant algorithms
- **September 2023:** MITRE contract awarded for support on deeper analysis and risk assessment
- **October 18, 2023:** Post-Quantum Cryptography Status Report for Director of OMB and Assistant to the President for National Security Affairs
- **Early 2024:** NIST to finalize standards for quantum-resistant algorithms and Administration to develop strategy on prioritized migration to quantum-resistant cryptography, with funding strategy
- **March 2024:** OMB PQC Plan of Action to Congress

Questions?

Dylan Presman
dylan.t.presman@ncd.eop.gov

Nick Polk
Nicholas.j.polk@omb.eop.gov