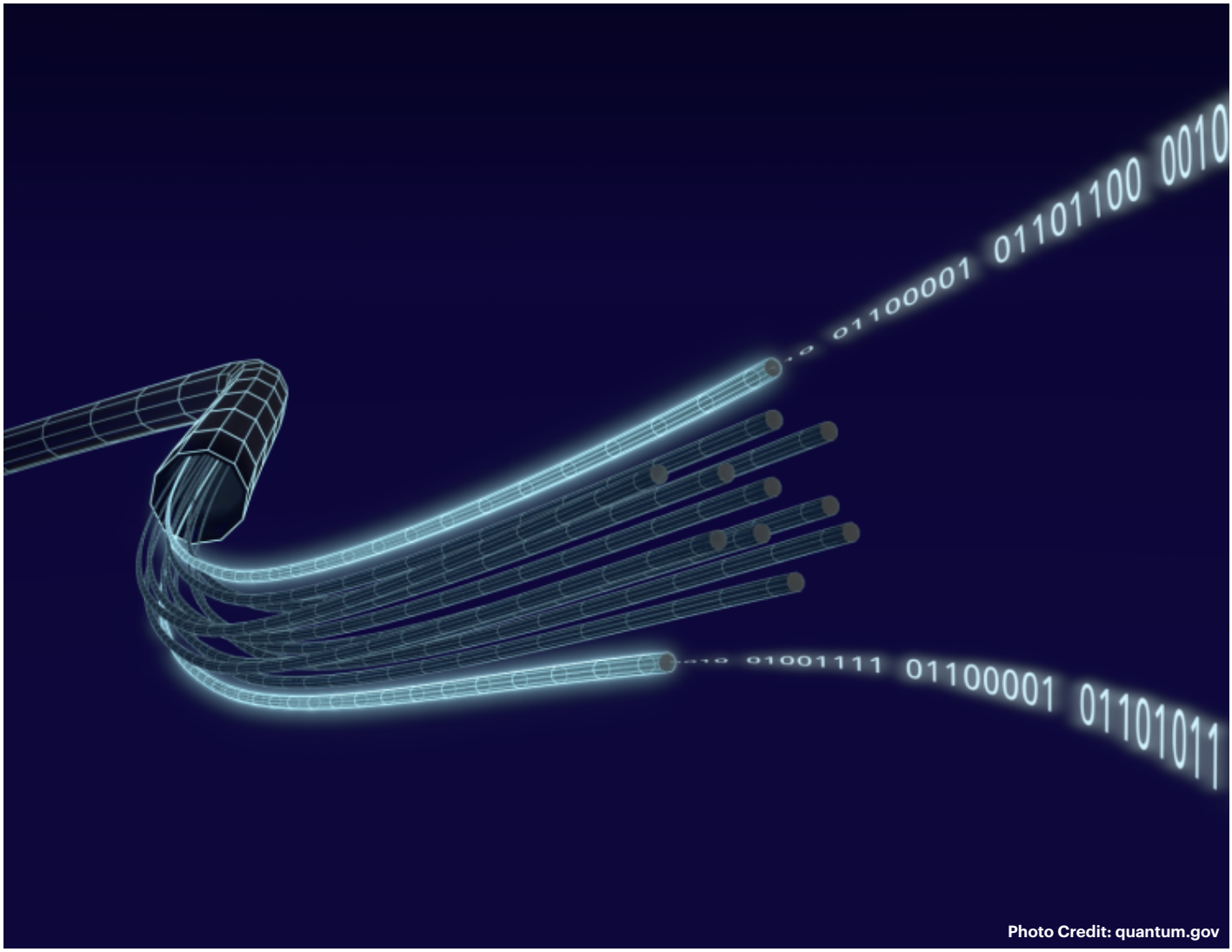


Photo Credit: quantum.gov

Executive Order 14412

SECURING THE NATION AGAINST ADVANCED CRYPTOGRAPHIC ATTACKS

By: James “Jimmy” Baker, Author & Public Sector Marketing Strategist

President Trump issued EO 14412 on June 22, 2026. **Future quantum computers will be powerful enough to break today's digital security encryption.** Even though these advanced computers do not fully exist yet, hackers are stealing and saving encrypted US data right now so they can unlock it later once the technology is ready. To defend the economy and national security, the US government is mandating a swift upgrade of federal computer networks to new, quantum-proof security standards, while helping private critical infrastructure companies do the same.

Summary

EO 14412

Key Findings

- **Risk:** Future large-scale quantum computers in the hands of foreign adversaries will disrupt current encryption.
- **Data:** Harvest now, decrypt later (HNDL). Threat actors will attempt to collect data now and decrypt at a later time with a quantum system.
- **Call to Action:** USA "must take steps to strengthen cryptographic protections for the Nation's sensitive data, critical infrastructure, and digital economy."

Time Line

- **July 22, 2026,** all federal agency heads must designate a PQC Migration Lead to oversee their cryptographic inventories and strategy.
- **September 20, 2026**, OMB will issue guidance directing each agency to review inventory of high value assets (HVA) and high-impact systems.
- **December 19, 2026,** initiate pilot project for post-quantum cryptography (PQC) migration by, and to be completed by December 31, 2027.
- **December 19, 2026,** submit a report to the President on the initial cryptographic assessment and strategy through the Committee on National Security Systems.
- **December 30, 2030,** transition all HVAs and high-impact systems to PQC for key establishment.
- **December 31, 2031,** transition all HVAs and high-impact systems to use PQC for digital signatures.

Quantum Computing

THE FUTURE OF TECHNOLOGY

Quantum computers, in the hands of hostile nation states and cyber criminals, pose a risk to the information technology enterprises and systems that enable the US Federal Government to provide services to citizens and protect our democracy. Quantum systems will have the ability to break and disrupt the public key cryptology currently used. An emerging market is developing for both for product and service companies in the public sector marketplace to help the government defend against the looming quantum threat.

With growing national attention on quantum computing and mandates requiring federal departments to prepare for quantum resiliency, this is an opportune time for product companies and system integrators to position themselves as trusted resources for the public sector.Many federal departments are involved in the National Quantum Initiative.

> ***Ongoing cyber activity against our Nation also presents the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum computers are operational. In light of these threats, the United States must take steps to strengthen cryptographic protections for the Nation's sensitive data, critical infrastructure, and digital economy.***
>
> **Executive Order 14412**

Recent Mandates, Policies, and Legislation

QUANTUM COMPUTING - A FEDERAL PERSPECTIVE

Over the last decade, the US Federal Government has issued multiple directives regarding the need for departments to migrate vulnerable systems and data to quantum-resistant cryptology. Whether you are a newcomer to the public sector marketplace or a seasoned veteran, the one constant is change. As the federal government begins to focus on post-quantum cryptology, your leadership, sales, marketing, and business development teams must familiarize itself with some new terms and policies currently impacting the federal government.

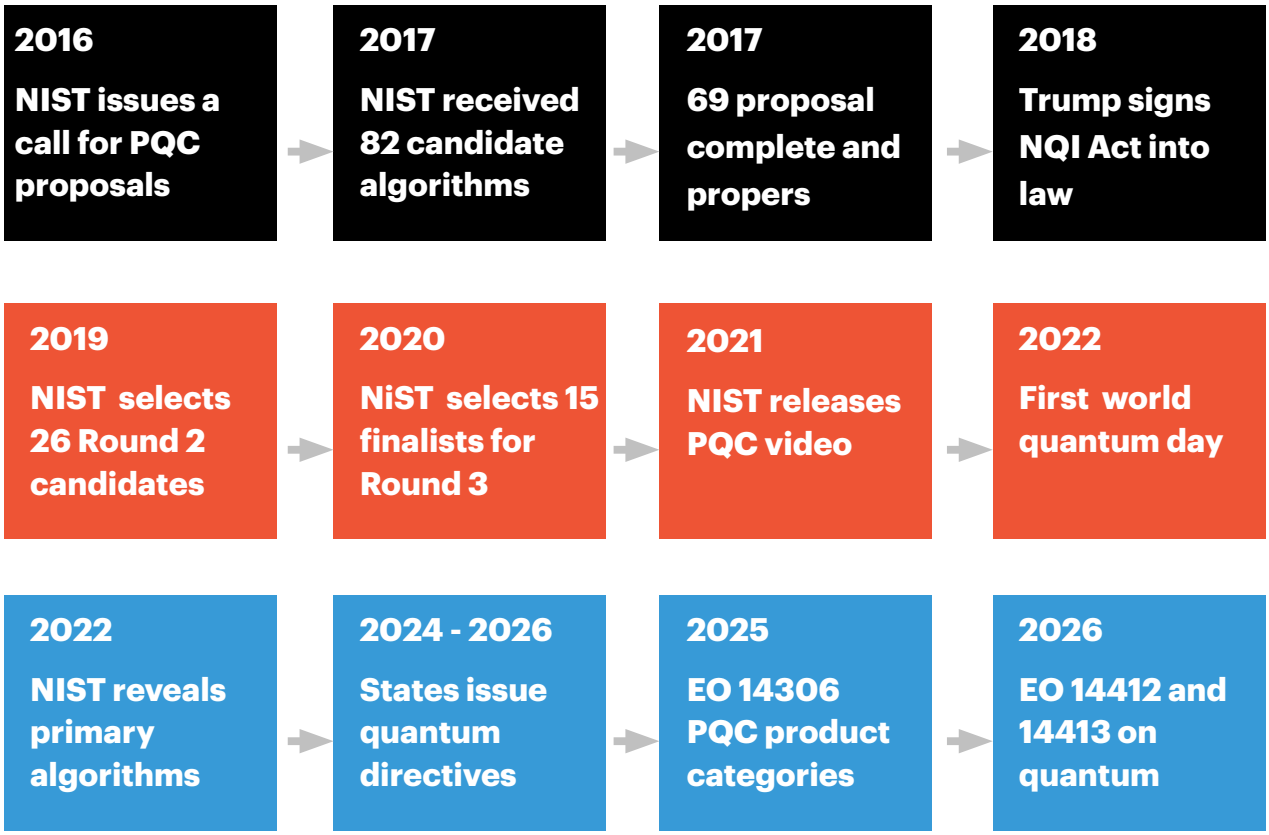


Figure 1

Classical Computing vs. Quantum Computing

A CLOSER LOOK

Classical computers are the systems used by government organizations for the last several decades. **Classical systems** are the computers we currently use that rely on bits to process and store information. **Quantum computing** is a type of nonclassical computing that operates in the quantum state through subatomic particles called **qubits.**

According to the NSA, "**Quantum computers** can, in principle, perform certain mathematical algorithms exponentially faster than a **classical computer**. In place of ordinary bits used by today's computers, quantum computers use qubits that behave and interact according to the laws of quantum mechanics. This quantum physics-based behavior would enable a sufficiently large-scale quantum computer to perform specific mathematical calculations that would be infeasible for any conventional computer."

The federal government incorporates **cryptology and cryptography** in its mandates and directives. **Cryptology** refers to using science in communications and the study of cryptography. In cybersecurity, **cryptography** is a way to secure and encrypt information and data through coding so that only the person the message was intended for can receive the information. NSA also stated, "**Quantum-resistant, quantum-safe, and post-quantum cryptography** are all terms used to describe cryptographic algorithms that run on standard encryption/decryption devices and are widely recognized by experts to be resistant to cryptanalytic attacks from both classical and quantum computers."

Conclusion and Path Forward

EO 14412

As your organization contemplates the emerging quantum marketplace, please consider the following factors.

- EO 14412 has time-bounded deliverables.
- PQC offers an opportunity to expand your security portfolio.
- Technology leaders such as Microsoft, IBM, Nvidia, Google, Amazon, and Intel are heavily investing in quantum computing.
- Many state and education organizations are creating quantum directives and institutions in California, Connecticut, Maryland, Illinois, Virginia and Texas. This means there is a play for PQC at both SLED and Federal levels.

The Quantum Journey Forward

With national attention on quantum computing as well as the mandates for federal departments to begin preparations for quantum resiliency through post-quantum cryptology, now is an opportunity for product companies and system integrators to position themselves to support the Fed and SLED quantum directives.

Let's Talk

Contact me to discuss how I can help your team create your quantum marketing strategy for public sector.

Email: james@jamesjbaker.com
Web: www.jamesjbaker.com
Mobile: 703.303.4233
Linked In: https://www.linkedin.com/in/jamesjbakerjr/