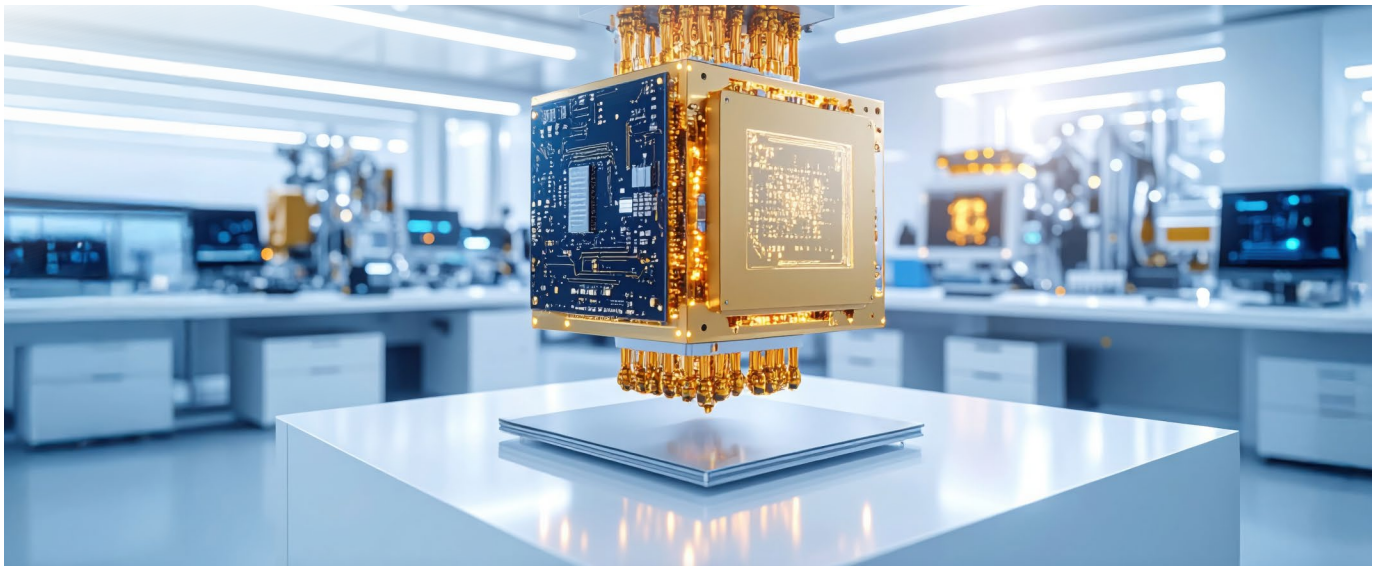
February
2026

QUANTUM COMPUTING THREATS TO CYBER SECURITY

JOB AID

CDSE Center for Development of Security Excellence



PURPOSE

Quantum computing represents a major shift in data processing capability. While it offers significant technological benefits, it also introduces serious risks to national security and counterintelligence operations. This Job Aid provides an overview of quantum computing, its development factors, associated threats, and current mitigation efforts.

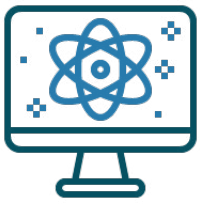
WHAT IS QUANTUM COMPUTING?

Quantum computing uses the principles of quantum mechanics to process information.

- Traditional computers use bits (0 or 1).
- Quantum computers use qubits, which can represent multiple states at once. A qubit (quantum bit) is the basic unit of quantum information, like a classical bit (0 or 1), but it can also be both 0 and 1 at the same time due to superposition.

SIMPLE COMPARISON:

Classical computer
reads one book at a time



Quantum computer
scans an entire library simultaneously

This allows quantum systems to evaluate many possible solutions at once, enabling massive speed and processing advantages.

FACTORS INFLUENCING QUANTUM COMPUTER DEVELOPMENT

Quantum technology has the potential to revolutionize computing, but also introduces new security challenges.

Key development factors policymakers have considered include:

- Encouraging public–private collaboration
- Expanding the quantum workforce
- Supporting continued research and investment
- Building a secure and resilient supply chain

These steps are critical to maintaining U.S. technological leadership while managing emerging risks.

NATIONAL SECURITY AND CRYPTOGRAPHIC THREAT

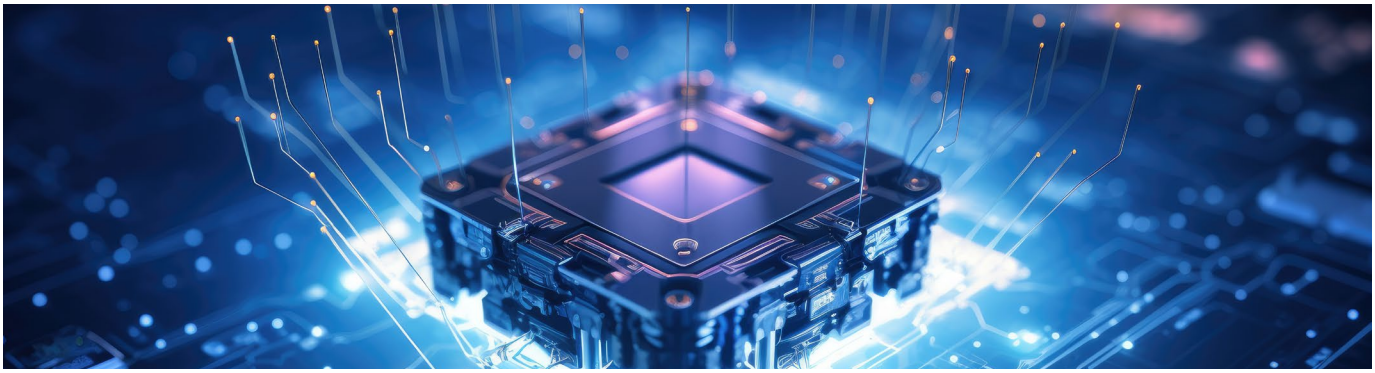
Quantum computers may eventually be capable of breaking widely used encryption methods that protect:

- Federal systems
- Critical infrastructure
- Sensitive government and commercial data

Experts estimate that quantum computers capable of breaking current public-key cryptography could emerge as soon as early-to-mid 2030's.

This creates a serious long-term risk, especially for information that must remain secure for decades.

Public-key cryptography is a security system using pairs of mathematically related keys—a publicly shared key for encryption or signature verification, and a corresponding private key kept secret for decryption or signing.



U.S. STRATEGY TO ADDRESS THE THREAT

Since 2018, multiple federal efforts have contributed to an emerging national strategy focused on post-quantum cryptography (PQC).

Three Primary Goals:

1. Standardize post-quantum cryptographic algorithms
   - Resistant to both classical and quantum attacks
2. Migrate federal systems
   - Transition government networks to PQC
3. Encourage nationwide preparedness
   - Across government, industry, and critical infrastructure sectors

Agencies leading these efforts include CISA, NSA, and the NIST.

WHY PREPARATION MUST BEGIN NOW

Cyber threat actors may already be collecting encrypted data today with the intent to decrypt it in the future — known as:

"Harvest now, decrypt later."

Because cryptographic migration is complex and time-consuming, organizations are urged to:

- Develop quantum-readiness roadmaps
- Conduct cryptographic inventories
- Perform risk assessments
- Engage vendors regarding quantum-ready solutions
- Plan to replace or update vulnerable public-key algorithms

Early planning reduces long-term operational and security risk.

QUANTUM KEY DISTRIBUTION (QKD)

Quantum Key Distribution (QKD) is a form of quantum cryptography that already exists today.

- Uses quantum physics to securely distribute encryption keys
- Works alongside traditional symmetric encryption algorithms
- Requires specialized hardware such as: control electronics, lasers, and microwave generators

Important distinction:

- QKD does not replace encryption systems
- It only distributes cryptographic keys

QKD is separate from quantum computers that, may one day threaten encryption.

KEY TAKEAWAYS

- Quantum computing offers powerful capabilities, but creates major security risks
- Current encryption methods may be vulnerable in the future
- Post-quantum cryptography is essential for long-term data protection
- Federal agencies and private organizations must begin planning now
- Early preparation reduces exposure to future quantum-enabled attacks

RESOURCES

- National Institute of Standards and Technology (NIST): Post-Quantum Cryptography Standardization Project
  https://www.nist.gov/quantum-information-science/quantum-computing-explained
- National Security Agency (NSA): Quantum Computing and Cryptography: CISA, NIST, and NSA
  https://www.nsa.gov
- Center for Strategic & International Studies (CSIS): Quantum Computing and National Security
  https://www.csis.org/analysis/quantum-computing-and-national-security
- U.S. National Counterintelligence and Security Center (NCSC): Annual Threat Assessments
  https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2025/4058-2025-annual-threat-assessment
- World Economic Forum: Why Quantum Computing is a Threat to Cybersecurity
  https://www.weforum.org/stories/2024/04/quantum-computing-cybersecurity-risks
- MIT Technology Review: The Race to Develop Post-Quantum Cryptography
  https://www.technologyreview.com