IBM Quantum Safe
→ Defense

IBM Quantum Safe for defense

Protect national and economic security with quantum-safe technology

National security in the quantum era

Quantum computing offers the potential for nations to gain competitive advantages, such as advances in pharmaceutical, materials science, and energy research. At the same time, the potential for a future cryptographically relevant quantum computer (CRQC) to be misused presents a significant risk to a country's national and economic security. Even before a CRQC becomes available, "harvest now, decrypt later" attacks could enable adversaries to steal sensitive data and store it until quantum computers become powerful enough to decrypt it, making it critical for government organizations to start planning and executing a transition to quantum-safe cryptography.

Cryptography is used by government entities and organizations supporting critical infrastructure to protect confidential data and communications. Many cryptographic protocols depend on public-key encryption algorithms (such as RSA, ECDH, and ECDSA), which are vulnerable to attack by a future CRQC. Even today, data that is not protected with quantum-safe cryptography is at risk of "harvest now, decrypt later" attacks, in which data is stolen and stored until a CRQC becomes available.

Understanding current and future risks

With nations vying for dominance in the race to develop quantum computers, the first quantum-enabled cyberattacks are likely to be executed by nation-state actors targeting high-value assets on government systems. As the US government warns, such attacks "could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."[1] The cascading damages could erode public trust in government and threaten national security.

For those in the defense industry, cryptographic vulnerabilities in the supply chain are of particular concern. Equipment programs and defense prime contracts have decades-long lifespans, driving urgency around quantum-safe cryptographic protections. To maintain continuous security despite fragmented regulations across countries, the use of legacy systems and third-party tools, and complex approval structures, it is critical for defense organizations to begin the transition to post-quantum cryptography. Integrating across domains (air, land, sea, space, and cyber), as recommended by the US National Defense Industrial Strategy,[2] will minimize the risk of operational disruption and enhance interoperability and crypto-agility. Nations with a clear quantum-safe mandate will not only be able to maintain a robust cryptographic risk posture, but they will also garner more trust in the geopolitical landscape.

What's at stake for defense organizations?

- **National security risks:** Classified military intelligence, diplomatic negotiations, and intelligence gathering could be compromised.
- **Economic damages and instability:** Critical infrastructure like power grids, financial systems, and communication networks could be undermined.
- **Loss of trust:** Personnel data, including Social Security numbers, medical records, and financial information could be exposed, causing military staff and the wider public to lose trust in the military.

Benefits of forward planning

While mandates may differ across borders, the United States has established a program for developing a post-quantum cryptography standard that many nations are expected to follow. In 2022—after six years and three rounds of evaluation—the US Department of Commerce's National Institute of Standards and Technology (NIST) announced the selection of four quantum-resistant cryptographic algorithms for standardization, three of which (CRYSTALS-Kyber, CRYSTALS-Dilithium, and Falcon) were contributed by IBM researchers. NIST expects to publish its post-quantum cryptography (PQC) standard in mid-2024.

Recognizing the importance of early planning, the US Federal Government has identified actions that executive departments and operators of national security systems (NSS) must take leading up to and following the publication of NIST's PQC standard. NSM-10 requires annual inventories of vulnerable cryptographic assets beginning in 2023 and advises agencies to begin testing commercial solutions that use pre-standardized quantum-safe cryptographic algorithms.[1] Additionally, the National Security Agency's Commercial National Security Algorithm Suite (CNSA) 2.0 establishes a timeline for NSS owners, operators, and vendors to migrate to quantum-resistant cryptography, with full compliance required by the early 2030s.[3] Beyond maintaining compliance, there are several advantages for defense agencies to begin their quantum-safe journey now:

Strengthen national security

- Ability to improve supply chain risk management through full-stack quantum-safe componentry
- Protection of defense and intelligence operations, diplomatic negotiations, and critical infrastructure
- Reputational benefits such as increased investments in and growth of operations

Mitigate digital divide consequences

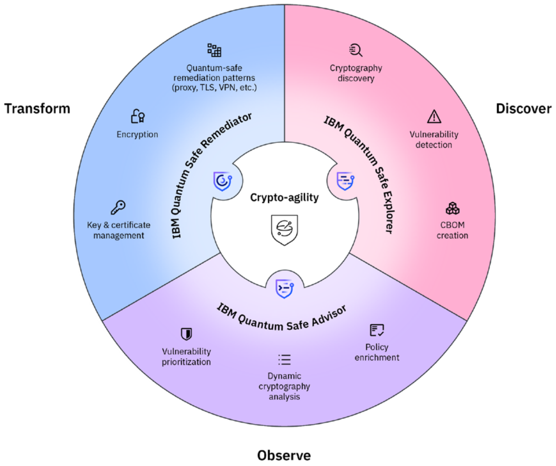
- Ability of teams to upskill in the new quantum-safe cryptographic algorithms and implementations
- Coordination on regulatory approaches to quantum-safe requirements across the global supply chain

Establish crypto-agility and quantum cyber resilience

- Opportunity to modernize cybersecurity architecture to align with the Zero-Trust Architecture mandate, CNSA 2.0, and the requirements laid out in NSM-10
- Enhanced crypto-agility through performance testing of PQC algorithms and scalable implementations

Building a robust quantum risk posture with IBM Quantum Safe technology

IBM Quantum Safe is a comprehensive set of technologies, services, and infrastructure that equips organizations to plan and execute an agile transition to quantum-safe cryptography.


Transform
Discover
Observe
Crypto-agility
IBM Quantum Safe Remediator
IBM Quantum Safe Explorer
IBM Quantum Safe Advisor
Quantum-safe remediation patterns (proxy, TLS, VPN, etc.)
Encryption
Key & certificate management
Cryptography discovery
Vulnerability detection
CBOM creation
Vulnerability prioritization
Dynamic cryptography analysis
Policy enrichment

With its cryptographic expertise, advanced cybersecurity analytics, and industry experience, IBM can support defense agencies and vendors throughout their quantum-safe journey, which includes the following key steps:

Identify applications and systems that depend on at-risk cryptography.

Analyze cryptographic risk posture to prioritize vulnerable data and systems.

Upskill teams in the capabilities needed to support the quantum-safe transition.

Test post-quantum encryption algorithms to optimize performance and to support the incremental mandating of adoption.

Establish a timetable and procedure for mandatory quantum-safe requirements by looking to NIST and collaborating with quantum-safe working groups.

Learn more about IBM Quantum Safe and start your journey to post-quantum resilience today: https://ibm.biz/BdM8DD

[1] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). Whitehouse.gov, May 4, 2022.

[2] National Defense Industrial Strategy. Department of Defense, October 27, 2022.

[3] CNSA Suite 2.0. National Security Agency, September 7, 2022.