August 2022

Preparing Critical Infrastructure for Post-Quantum Cryptography

Quantum Risk to Digital Communications

Nation-states and private companies are actively pursuing the capabilities of quantum computers. Quantum computing opens up exciting new possibilities; however, the consequences of this new technology include threats to the current cryptographic standards. These standards ensure data confidentiality and integrity and support key elements of network security. While quantum computing technology capable of breaking public key encryption algorithms in the current standards does not yet exist, government and critical infrastructure entities—including both public and private organizations—must work together to prepare for a new post-quantum cryptographic standard to defend against future threats.

In March 2021, Secretary of Homeland Security Alejandro N. Mayorkas outlined his vision for cybersecurity resilience and identified the transition to post-quantum encryption as a priority. Government and critical infrastructure organizations must take coordinated preparatory actions now to ensure a fluid migration to the new post-quantum cryptographic standard that the National Institute of Standards and Technology (NIST) will publish in 2024.

Conducting an inventory of vulnerable critical infrastructure systems across the 55 National Critical Functions (NCFs) is the first step of this preparation and is included in the Post-Quantum Cryptography Roadmap developed by DHS and NIST. There are potential risks from quantum computing to each of the 55 NCFs. CISA urges asset owners and operators to follow the Roadmap and CISA's Post-Quantum Cryptography Initiative webpage to begin the process of addressing this risk within their organization.

The Quantum Threat to Public Key Cryptography

All digital communications—email, online banking, online messaging, etc.—rely on data encryption built into the devices and applications used to transmit data. This encryption is based on mathematical functions that secure data in transit, protecting the data from tampering or espionage. In public key encryption (also known as asymmetric encryption), the mathematical functions rely on cryptographic keys to encrypt data and authenticate the sender and recipient.

Public key encryption requires that each message use two separate, but related keys (one is called a public key and the other is called a private key) to protect data. The sender and recipient of the data do not share their private keys, while public keys can be shared without downgrading the level of cryptographic security. The sender uses their private key to encode the message and provides the recipient with their public key to decode the message. To reply, the recipient will follow the same procedure and share their public key.

Because only two keys can decode a message, digital signatures allow a party to sign a message with their private key while verifiers use the public key to authenticate that the sender actually sent the message. All organizations regularly use public key cryptography to securely send emails, verify digital signatures, secure sensitive data, and protect user information online.

When quantum computers reach higher levels of computing power and speed, they will be capable of breaking public key cryptography, threatening the security of business transactions, secure communications, digital signatures, and customer information.

Experts currently believe that quantum computers are less likely to impact symmetric key cryptography in which the sender and receiver use the same key to protect data. Rather than requiring quantum-resistant algorithms, symmetric key cryptography can mitigate the threat posed by quantum computing—and maintain the same level of security as it currently provides—by using longer key sizes.

What Is Quantum Computing and How Is It a Threat?

Quantum computers leverage the properties of quantum physics to derive computing capabilities that are different and, in some ways, far exceed those of classical computers. By leveraging quantum mechanics, quantum computers utilize qubits, or "quantum bits," rather than binary bits, to achieve greater computing power and speed for specific scenarios—such as breaking current public key encryption.

The algorithms that underpin the current encryption standards rely on solving mathematical problems that classical computers cannot reasonably solve. Because of their expense and physical size, quantum computers that can break encryption algorithms are likely to first be developed for use by technology companies, research institutions, or nation-states. In the hands of adversaries, sophisticated quantum computers could threaten U.S. national security if we do not begin to prepare now for the new post-quantum cryptographic standard.

Potential Impacts to National Critical Functions

NCFs are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or a combination thereof (see National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems). To help critical infrastructure partners prepare for the adoption of post-quantum cryptography, CISA analyzed how each of the 55 NCFs is vulnerable to quantum computing capabilities. CISA also analyzed the challenges NCF-specific systems may face when migrating to post-quantum cryptography. The results of this analysis identified the urgent vulnerabilities and NCFs that are most important to address first to enable a successful migration to post-quantum cryptography.

CISA analyzed each NCF based on its vulnerability to the expected impacts of quantum computing on the nation's critical infrastructure. CISA ranked each NCF as high, medium, or low priority based on the urgency of its dependencies on the current cryptographic standards, the scope and scale of organizations and systems that will require updates, and the relative costs to organizations to upgrade to the new standard. CISA also ranked factors impacting each NCF's migration as exacerbating, neutral, or mitigating. These factors include availability of human capital and status of migration preparations.

Prioritizing NCFs for Stakeholder Engagement

An assessment developed for CISA by the Homeland Security Operational Analysis Center (HSOAC)[1] identified three NCF areas that the U.S. government and private industry should prioritize:

1. Several NCFs will enable the migration of most other functions to post-quantum cryptography. Success in providing this support will mitigate much of the risk for most users.
2. The dependence on industrial control systems (ICSs) is an area of concentrated vulnerability because of the long replacement life cycle of ICS hardware and wide geographic distribution of equipment.
3. NCFs with especially long secrecy lifetimes will require significant support to ensure that the nation's most sensitive data remains fully secured.

CISA will also continue to provide insight on how quantum computing capabilities impact NCFs going forward.

NCFs That Will Enable Post-Quantum Migration

Several NCFs will directly support the migration to post-quantum cryptography across the critical infrastructure community by providing products, patches, and other software and firmware updates that integrate the new cryptographic standard. Most NCFs and the critical infrastructure they support depend on these enabling functions to successfully execute the migration and keep their sensitive information secure. The following four NCFs are likely to be the most important in supporting successful migration:

- Provide Internet-Based Content, Information, and Communication Services
- Provide Identity Management and Associated Trust Support Services
- Provide Information Technology Products and Services
- Protect Sensitive Information

CISA recommends that stakeholders responsible for these NCFs partner closely with NIST, DHS, and other government agencies to ensure their preparedness to not only migrate themselves, but also to support the

[1] HSOAC is a federally funded research and development center operated by the RAND Corporation.

migration of digital communications across other NCFs. Action will be required of stakeholders across all NCFs, but only after these four create products and services that enable further updates to take place.

Industrial Control Systems

Upgrading ICSs to post-quantum cryptography will be a challenge because deployed cryptography-dependent ICS hardware is costly, and the associated equipment is often geographically dispersed. However, organizations should make necessary preparations for migration to post-quantum cryptography. CISA urges ICS organizations to ensure that their hardware replacement cycles and cybersecurity risk management strategies account for actions to address risks from quantum computing capabilities.

Supporting Long Secrecy Lifetimes

NCFs that depend on data confidentiality over long time frames are uniquely vulnerable to quantum challenges, including catch-and-exploit campaigns in which adversaries capture data that has been encrypted using current encryption algorithms and hold on to such data with the intention of decrypting it when a quantum computer capable of breaking the encryption is available.

Organizations with a long secrecy lifetime for their data include those responsible for national security data, communications that contain personally identifiable information (PII), industrial trade secrets, personal health information (PHI), and sensitive justice system information.[2] While many NCFs are potentially vulnerable to catch-and-exploit campaigns, practical challenges can inhibit adversaries from executing most campaigns successfully. For example, organizations typically store data with a long secrecy lifetime on internal networks and rarely transmit it, which limits its vulnerability. However, such security controls are not foolproof, and organizations should prioritize security for these NCFs to prevent catch-and-exploit operations.

NCFs that Depend on ICS

- Generate Electricity
- Distribute Electricity
- Transmit Electricity
- Transport Cargo and Passengers by Rail
- Transport Cargo and Passengers by Vessel
- Transport Materials by Pipeline
- Transport Passengers by Mass Transit
- Manage Hazardous Materials
- Manage Wastewater
- Store Fuel and Maintain Reserves
- Exploration and Extraction of Fuels
- Fuel Refining and Processing Fuels
- Manufacture Equipment
- Produce and Provide Agricultural Products and Services
- Produce and Provide Human and Animal Food Products and Services
- Produce Chemicals
- Provide Metals and Materials
- Supply Water

NCFs with Long-Term Confidentiality Needs

- Provide Internet-Based Content, Information, and Communication Services
- Protect Sensitive Information
- Provide Satellite Access Network Services
- Support Community Health
- Provide Wireless Access Network Services
- Provide Information Technology Products and Services
- Enforce Law
- Provide Material and Operational Support to Defense
- Maintain Access to Medical Records

Recommended Actions for Leaders

Although NIST will not publish the new post-quantum cryptographic standard until 2024, CISA urges leaders to start preparing for the migration now by following the Post-Quantum Cryptography Roadmap. Do not wait until the quantum computers are in use by our adversaries to act. Early preparations will ensure a smooth migration to the post-quantum cryptography standard once it is available. **Note:** Organizations should wait until the official release to implement the new standard in a production environment.

Additional Resources

- CISA: Post-Quantum Cryptography Initiative webpage
- CISA: Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats
- CISA Press Release: CISA Announces Post-Quantum Cryptography Initiative
- RAND: Preparing for Post-Quantum Critical Infrastructure: Assessments of NCF Quantum Computing Vulnerabilities
- NIST: Migration to Post-Quantum Cryptography
- NIST: Getting Ready for PQC: Exploring Challenges Associated with Adopting and Using PQC Algorithms
- NIST: Status Report on the Third Round of NIST Post-Quantum Cryptography Standardization Process
- Canadian Centre for Cyber Security (CCCS): Addressing the quantum computing threat to cryptography
- CCCS: Preparing your organization for the quantum threat to cryptography

[2] **Note:** According to an assessment developed for CISA by HSOAC, the Operate Government NCF is "[t]o a significant degree . . . a collection of functions from other NCFs" that are included on the list, NCFs with Long-Term Confidentiality Needs.