RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

G7 FRANCE ÉVIAN 2026

GROUPE DE TRAVAIL CYBERSÉCURITÉ

CYBERSECURITY WORKING GROUP

Preparing for the Post-Quantum Era: A Call to Action

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Federal Office for Information Security

With the participation of the EU Commission -
supported by the EU Agency for Cybersecurity (ENISA)

We, the G7 Cybersecurity Working Group, recognize the growing threat that quantum computing poses to public-key cryptography, and the security of both public and private organizations. Although the exact timeline is uncertain, several recent advances suggest an anticipation of the development of quantum computers able to break widely used public-key cryptography mechanisms and threaten the security of digital infrastructures.

To address these risks, we must reframe the quantum threat from a distant future problem to a near-term threat that demands action across all sectors, not just critical infrastructure. Post-quantum cryptography (PQC) is a new field of cryptography, designed to be resistant to both classical and quantum cryptographic attacks, that can safeguard organizations from both the conventional cyber threat and the quantum threat. For this reason, governments and organizations should begin their PQC transition as soon as possible to avoid exposure to quantum risks and to provide a level of long-term protection of confidential data.

We acknowledge that transitioning to PQC is not a problem for individual organizations to solve in isolation, but rather a collective transition that can only be achieved with early engagement, coordinated planning, and informed decision-making across the public and private sectors.

This publication aims to highlight some of the risks that can be posed by cryptographically relevant quantum computers (CRQCs)[1] and to reaffirm our collective efforts to addressing this threat. It identifies five priority areas for PQC migration and highlights initiatives that G7 countries have advanced, in whole or in part, to encourage timely measures today and inspire other countries to take similar actions.

1. Cryptographically relevant quantum computers (CRQCs) are computers that are powerful enough to solve factorization and discrete logarithm problems of sizes that are used in quantum-vulnerable cryptography today.

WHY ACTION CANNOT WAIT

As quantum computing advances, the threat to public-key cryptography grows, making the transition to PQC an urgent priority that organizations can no longer afford to postpone.

Once CRQCs become available to threat actors, organizations will be at risk. Therefore, the transition to PQC is essential to protect organizations, confidential data, authentication mechanisms, and critical assets. The transition to PQC being a long process, it is essential for organizations to acknowledge the risks and the necessity of preparing their transition now.

Even though estimates for the availability of a CRQC vary, key risks exist today. Malicious cyber actors can already intercept and store encrypted data protected by public-key cryptography. This attack is known as "store now, decrypt later" or "harvest now, decrypt later" and is relevant where confidentiality of information must be protected for longer than the time required to develop a CRQC (for instance governmental data, sensitive personal data, trade or business secrets). This means that organizations may already be exposed to the threat today.

Malicious cyber actors with access to CRQCs will also be able to target authentication mechanisms that help provide assurance and help protect the integrity of data between communicating parties and the integrity of devices. This capability could allow malicious cyber actors to impersonate trusted entities, compromise equipment, forge trusted data, or access confidential data, therefore undermining confidence in secure communications or contractual agreements.

Because supply chain risks can cascade and compromises to authentication can allow immediate lateral movement, the vulnerabilities of one organization may expose other organizations and sectors to these risks.

To protect themselves from the threat brought by CRQCs, organizations should begin planning their PQC transition now and should aim to complete their transitions within any the timelines set out by their national cybersecurity authorities. In addition to quantum-related risks, organizations that delay their PQC transition may lose competitive advantage or may be excluded from contracting opportunities, including public procurement.

To mitigate risks, governments and organizations should first identify systems that hold the most critical data and assets and prioritize PQC transition efforts accordingly. Acting proactively, rather than waiting for confirmed CRQC availability, is important to managing quantum risk.

As proposed in the *G7 Cybersecurity Working Group Statement on preparing for a post-quantum cryptography migration*[2], organizations should: adopt a phased and risk-based strategy; start their PQC transition early; inventory their cryptographic assets; map their dependencies; and develop a transition plan. To limit transition-related costs, they should opt to purchase products that integrate PQC and replace their systems with quantum-safe ones as part of their standard renewal schedule. As such, starting the transition early could result in lower migration costs overall. Planning and conducting their PQC transition properly[3] would enable organizations to prevent insecure implementations and avoid increased exposure to conventional cyber threats.

Achieving a timely and effective transition to PQC requires coordinated action across governments and industry. While organizations must act now to mitigate their own risks, governments play a critical role in creating the conditions for scalable, secure, and interoperable adoption. Organizations are already implementing actions to support this transition, although the scope and pace of these efforts remain closely linked to the infrastructure, regulatory environment, and technological maturity of each country.

In this context, the G7 countries are individually advancing some, or all, of the initiatives in the five priority areas listed below. Each area includes key considerations to take into account when implementing one or more of them.

- **Raising awareness:** The quantum threat remains off the radar for many organizations and not properly resourced, with other security concerns taking precedence. Yet, a successful and collective transition to PQC can only be achieved if organizations understand that the quantum threat is an economic and business risk, and not merely a cryptographic risk. To address this lack of awareness, the benefits of PQC and the risks it mitigates can be highlighted by launching awareness campaigns, providing technical guidance, and encouraging the upskilling of organizations. Strategies relating to raising awareness should align with wider strategies for managing cyber risk.

---

2. G7 Cybersecurity Working Group Statement on preparing for a post-quantum cryptography migration - Canadian Centre for Cyber Security

3. Organizations can follow recommendations provided by the G7 Cybersecurity Working Group statement on preparing for a Post-quantum Cryptography Migration but should refer to their national guidelines and cybersecurity agencies for additional information.

• **Developing national strategies:** National strategies on transitioning to PQC should aim at both attaining an adequate supply of PQC hardware and software products and encouraging users to adopt them. The transition to PQC should also be considered in broader initiatives, including security and digital privacy strategies.

• **Research and development:** Research and development efforts should focus on advancing PQC through innovation and the development of practical solutions. These can include funding programs for research and development of PQC and supporting pilot projects and testbeds for organizations transitioning to PQC.

• **Developing public-private partnerships:** Cooperation between government, industry, and academia is a key factor to support coordinated transition efforts. The G7 Cybersecurity Working Group recommends those partnerships be aimed at developing domestic expertise and industry capabilities in quantum-safe technologies; such measures may help reduce the cost of PQC transition. The Working Group also recommends countries encourage collaboration between organizations within and across sectors to share resources, expertise, insights, and the development of playbooks and case studies.

• **Integrating PQC into cybersecurity requirements:** Countries should treat PQC adoption as a foreseeable evolution of cryptographic best practices rather than a standalone compliance obligation. Furthermore, introducing specific requirements within the framework of public procurement can encourage organizations to initiate the transition, both for the products and services they offer on the market and within their own operations.

CONCLUSION

Tackling the risks that the impending quantum computing era poses to current cryptographic systems, and ultimately organizations in which they are embedded, requires a coordinated global effort to transition to PQC. To strengthen collective resilience and safeguard confidential data, supply chains, and critical systems, public and private organizations must jointly act now. The transition to PQC is the key foundation to help build a secure and resilient digital future.

SEPTEMBER 2026

France's Cybersecurity Agency
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr