The Canadian Approach to Quantum-Safe Cryptography
David Sabourin
Canada has a new National Cyber Security Strategy


**National Cyber Security Strategy**

- **Secure and Resilient Canadian Systems**
  - Protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems

- **An Innovative and Adaptive Cyber Ecosystem**
  - Support advanced research, foster digital innovation, and develop cyber skills and knowledge

- **Effective Leadership, Governance, and Collaboration**
  - Collaborate with provinces, territories, the private sector, as well as international allies, to take a leadership role in advancing cyber security
The Canadian Centre for Cyber Security

- A key initiative of the new Cyber Strategy

- Flagship cyber security authority for Canada, demonstrating Federal leadership and clarity to stakeholders across Canada

- Unites cyber security expertise across the Government of Canada into a single window for stakeholders

- Governments
- Critical Infrastructure
- Private Industry
- Academia
- Canadian Public
- International Partners
Program Integration

The Cyber Centre consolidates all GC cyber security operations into one unique, innovative, and forward-looking organization, as part of CSE.

- Canadian Cyber Incident Response Centre and GetCyberSafe (PS)
- Security Operations Centre (SSC)
- IT Security branch (CSE)
Functions include

- Expert advice and guidance
- Secure solutions and services
- Cyber security training and education

Making Canada Quantum Safe
Quantum Technologies and Cryptography

Quantum Computers
- Can do computations that are infeasible for today’s computers
- Very good at solving some problems
- Cryptographically relevant quantum computers may be viable by the 2030s

Quantum Communications
- Securely transmitting messages using quantum channels
- Quantum Key Distribution
- Quantum Random Number Generation
  - Quickly produced, quantum-safe

Field developing rapidly
Not yet mature technologies
Quantum Computers: Impact now and in the future

**Impact Now:** Information with a long lifespan could be collected, stored, then decrypted in the future: *threat to confidentiality.*

**Future Impact:** Once a large quantum computer is built, the cryptography used to verify the source and integrity of information will be broken: *threat to authentication.*
CCCS Quantum Security Activities

Our efforts are twofold:

Protecting our most sensitive information today

- Long-lifespan information
- Work with information owners to understand the impact to their information
- Provide guidance and assistance on how to protect against the quantum threat today

Developing a long-term strategy for the future

- Partnering with Academia, Industry and Standards organizations
- Advancing quantum-safe research, solutions, and technologies
- Promoting awareness and planning and cryptographic agility
- Lead the development of a Canadian cryptographic community-backed strategy for a secure online Canada
Conclusions

- Information with a long life is at risk now, but there are steps that can be taken today to protect it.
- The cryptographic community including governments, academia and industry are taking steps to develop, standardize and implement quantum-safe cryptographic solutions.
- Prioritizing cryptographic agility will help enable the transition to quantum-safe cryptography.
The Canadian Centre for Cyber Security

www.cyber.gc.ca