CANADIAN CENTRE FOR
CYBER SECURITY

How the Canadian Government is Preparing for PQC

PKI Consortium

Post-Quantum Cryptography Conference

March 2023

The Canadian Centre for Cyber Security

- A clear, trusted source of relevant cyber security information for Canadians
- We provide targeted cyber security advice and guidance to protect the country's most important cyber systems
- We work with private sector partners to solve Canada's most complex cyber challenges - cyber defence is a team sport.
- We develop and share our specialized cyber defence technology and knowledge
- We lead the Government's operational response during cyber events

What We Do

SINGLE SERVICE WINDOW	**INCLUSIVE LEARNING AND INNOVATION HUB**	**INTEGRATED INCIDENT RESPONSE**	**EXPERT ADVICE AND GUIDANCE**
			
CRITICAL INFRASTRUCTURE ENGAGEMENT PROGRAM	**COMMERCIAL AND GOVERNMENT CRYPTOGRAPHIC EQUIPMENT ASSURANCE**	**DEFENDING GOVERNMENT NETWORKS AND SYSTEMS FROM CYBER THREATS**	**INFORMATION AND TECHNOLOGY SHARING WITH THE PRIVATE SECTOR**
			

Outline

- Activities to ensure the availability of quantum-safe solutions
- US federal government directives for PQC transition
- The Government of Canada (GC) landscape
- Why not deploy PQC now?
- Considerations on the use of hybrid PQC
- Recommendations and expected timeline

All GC departments will have a role in the PQC transition.
This presentation represents the Cyber Centre's views as the technical authority on cyber security and cryptography for the GC.

Ensure the Availability of Quantum-Safe Solutions

- Studying post-quantum cryptography (PQC) to have confidence in the security of the NIST selections
- Participating in standards activities related to the adoption of PQC
- Monitoring developments in quantum technologies and providing guidance on the quantum threat and the necessary cryptographic transition
- Participating in GC initiatives with respect to quantum communications and monitoring industry and government experiments in order to advise on the potential future use for cyber security

US Directives on the Quantum Threat

- Two White House National Security Memorandums (NSM) were issued in early 2022 related to the protection of US government systems against the quantum threat
- NSM-8 (January 2022) gave directives for use of NSA-approved PQC for US National Security Systems (NSS), i.e. systems containing classified and/or sensitive information critical to military or intelligence activities

NSM-10 (May 2022)	Quantum Computing Cybersecurity Preparedness Act (Dec 2022)

• NIST and CISA to lead PQC transition efforts for Non-NSS
  • NIST will propose a timeline to deprecate quantum-vulnerable cryptography within the next decade
  • *Within 1 year*, US Gov agencies must have a plan for upgrading non-NSS IT systems to use PQC
• US federal agencies shall not procure commercial PQC solutions in advance of NIST standards
	• *June 2023*: Guidance will be given to federal agencies on migrating to PQC (inventory and prioritization)
	• *Dec 2023*: Federal agencies to provide their inventory and prioritization to the OMB, CISA, and White House
	• *Within 1 year of NIST PQC standards*: Agencies to plan how to migrate IT systems inline with their prioritization
	• *April 2024*: OMB is to submit a federal IT migration strategy and funding estimate
	• *June 2024*: OMB to provide ongoing reports on the progress of federal agencies in the PQC migration

Government of Canada Landscape

Canada's highly-sensitive systems are integrated with allies

- We are aligned with the migration timelines issued by the US due to our close cooperation and equipment supply chain

Many of the GC's less-sensitive IT systems are centrally-managed

- Unique among our allies, Shared Services Canada handles IT across the GC
- Internal IT management committees bring together cyber security experts, policy makers, and IT administrators to discuss how to improve the GC's digital resilience and cyber security

GC is building partnerships with organizations in Canada's critical infrastructure

- Canada's CI sectors have fewer operators than our allies, enabling a close cooperation
- Leverage cyber security actions under the *National Strategy for Critical Infrastructure* and/or the *National Cyber Security Strategy*

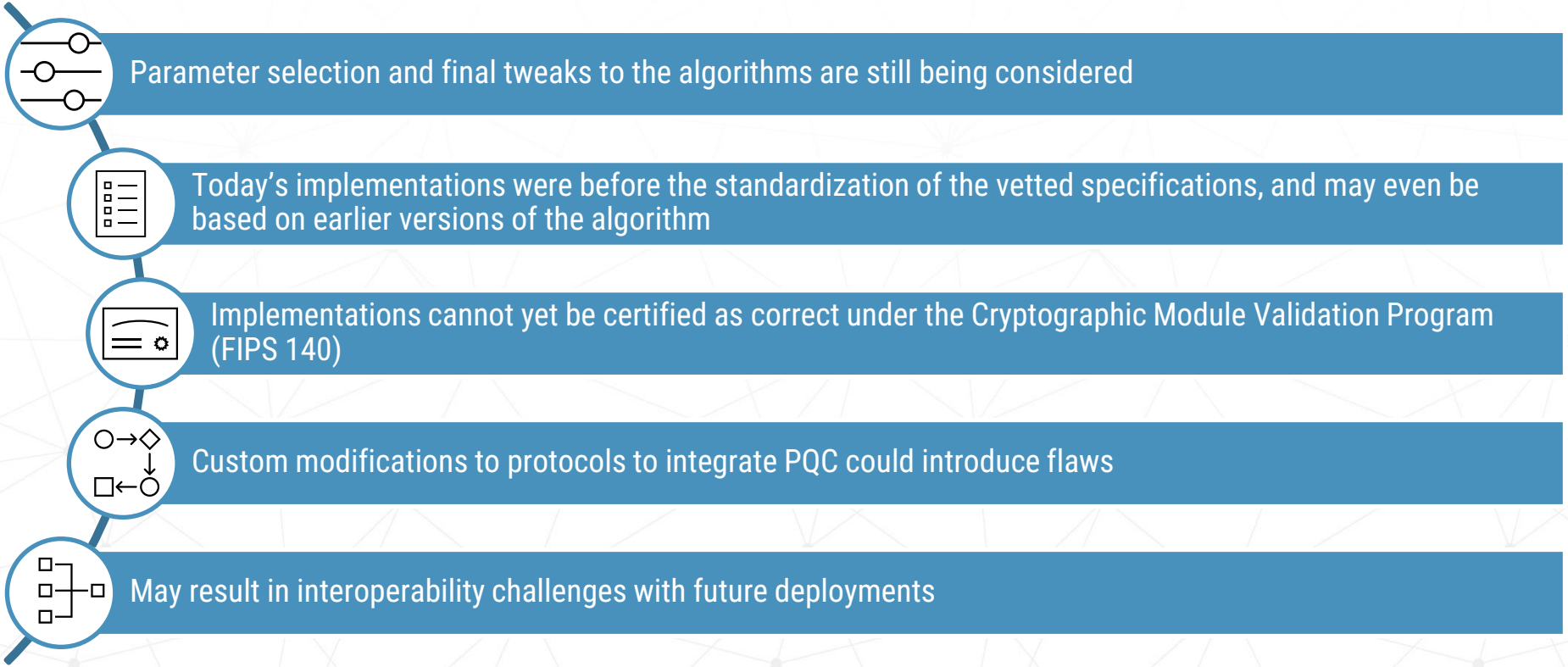
Plan for Protecting GC IT Systems

Efforts to identify and inventory GC cryptographic systems are ongoing

GC procurement language has been updated to ensure vendors are aware of the need to provide quantum-safe cryptography once CCCS guidance advises to do so

CCCS will update our cryptographic guidance when the standards are available and vendors can offer certified products with validated PQC

Risks in Early Adoption of PQC



Considerations on the Use of Hybrid PQC

Benefit	*Considerations*
Risk mitigation	• If the PQC algorithm has a flaw, then a hybrid PQC + classical does not have post-quantum security • Hybrid PQC + PQC will require a future transition if there is a desire to improve efficiency • Additional complexity, particularly with authentication • Layered solutions provide broader protection, but at increased cost
Ease the transition	• May not be needed in negotiated protocols • Downgrade protection is required • Future transition to remove the classical fallback
Policy compliance	• Jurisdictions may have specific cryptographic policies that do not share the same PQC • Hybrid may allow communications to satisfy both policies
Protocol integration	• DoS protection in IKEv2

- Standards organizations are still considering how hybrid could be used
- System owners will need to make a policy decision on when to use hybrid
- GC has not yet made a decision on where hybrid PQC should be used

Current Recommendations within GC

- Evaluate the sensitivity of your organization's information and determine its lifespan to develop a quantum risk assessment
- Determine the IT supplier for products or services protecting information at risk
  - Develop a transition plan for enterprise-managed IT systems to become quantum-safe, adopting cryptographic agile products and practices where possible (see ITSAP.40.018)
  - Engage with SSC and cloud service providers (CSPs) on roadmaps for externally-managed IT systems to become quantum-safe
- Ensure use of the GC procurement requirements for cryptographic products
  - Ask CCCS for technical advice if required

Do not adopt PQC in production systems
until recommended in ITSP.40.111

Expected Timeline for the Transition

"Now is not the time to panic, it is the time to plan." – Troy Lange (NSA) at ICMC 2022

CONNECT WITH US


@cse_cst


contact@cyber.gc.ca


www.cyber.gc.ca


@cybercentre_ca