Centre for International
Governance Innovation

SPECIAL REPORT

Canada's Migration to Post-Quantum Cryptography: Public-Private Roles

Ria Chakraborty, Kim de Laat and Raymond Laflamme

Centre for International
Governance Innovation

SPECIAL REPORT

Canada's Migration to Post-Quantum Cryptography: Public-Private Roles

Ria Chakraborty, Kim de Laat and Raymond Laflamme

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Research Director, Transformative Technologies Tracey Forrest
Director, Program Management Dianna English
Program Manager Grace Wright
Publications Editor Susan Bubak
Manager, Publications Jennifer Goyder
Graphic Designer Sepideh Shomali

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Ria Chakraborty is a graduate researcher in the quantum information science program at the University of Waterloo's Institute for Quantum Computing (IQC). Her work examines the governance, defence and security implications of quantum technologies to inform policy development. Ria holds a B.Sc. in mathematical physics from the University of Waterloo. During her undergraduate studies, she contributed to physics research at TRIUMF's Hyper Kamiokande neutrino experiment and worked with IQC groups on trapped ion systems as well as on the quantum encryption satellite. She also completed a research term at the Bank of Canada, assessing cryptocurrency vulnerabilities to quantum attacks and mapping options of existing quantum-safe cryptocurrencies for a future central bank digital currency.

Her policy journey began as an intern at the Office of the Superintendent of Financial Institutions, where she learned about technology-driven risks to Canada's financial system along with contributing to broader policy projects. Subsequently, she joined Innovation, Science and Economic Development Canada (ISED) while Canada's National Quantum Strategy was being rolled out. At ISED, she profiled the domestic quantum ecosystem and evaluated policy and governance frameworks. Currently, Ria is a Department of National Defence Quantum MINDS Scholar (part of QUANTUM NOW), advancing policy frameworks for defence applications and broader innovation in quantum technologies.

Kim de Laat is an assistant professor of organization and human behaviour at the University of Waterloo's Stratford School of Interaction Design and Business. As a sociologist of work and culture, she studies how inequality and uncertainty are structured in creative and knowledge-based organizations, with particular attention to their implications for gender equity. Her research has appeared in leading academic outlets such as the *ILR Review*, *Work and Occupations*, the *Socio-Economic Review* and *Work, Employment and Society*. Her recent article on remote work and gender inequality was a 2024 Rosabeth Moss Kanter Award Nominee for Excellence in Work-Family Research.

Committed to bridging research and public policy, Kim has worked with the National Research Council, Employment and Social Development Canada, and The Dais (formerly the Brookfield Institute for Innovation and Entrepreneurship) on initiatives related to diversity, equity and inclusion in the future of work. Her policy writing has appeared in such outlets as The Conversation, *The Globe and Mail*, *The Lancet* and *Policy Options*, among others. She is currently principal investigator of a Social Sciences and Humanities Research Council-funded study on hybrid work and cognitive labour, and an active contributor to ongoing policy discussions about work, technology and gender inequality.

Acknowledgement

The authors would like to acknowledge the late Raymond Laflamme, without whom this work would not have been possible. A pioneering figure in quantum information science, he not only advanced the field but also championed the integration of quantum technologies into public policy to promote responsible innovation. His mentorship, vision and leadership were foundational to the conception and success of this project.

Acronyms and Abbreviations

5G	fifth-generation
AI	artificial intelligence
ATM	automated teller machine
BSI	*Bundesamt für Sicherheit in der Informationstechnik*
CAVP	Cryptographic Algorithm Validation Program
CDL	Creative Destruction Lab
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
CISOs	chief information security officers
CMVP	Cryptographic Module Validation Program
CRQCs	cryptographically relevant quantum computers
CSE	Communications Security Establishment
DND	Department of National Defence
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
FRFIs	federally regulated financial institutions
G7	Group of Seven
GAO	Government Accountability Office
GDPR	General Data Protection Regulation
GRI	Global Risk Institute
IoT	Internet of Things
IPR	intellectual property rights
IRAP	Industrial Research Assistance Program
ISED	Innovation, Science, and Economic Development Canada
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
NCFs	National Critical Functions
NIST	National Institute of Standards and Technology
NQS	National Quantum Strategy
NSA	National Security Agency
NSM	National Security Memorandum
NVLAP	National Voluntary Laboratory Accreditation Program
OSFI	Office of the Superintendent of Financial Institutions
OT	operational technology
PIPEDA	Personal Information Protection and Electronic Documents Act
PKC	public-key cryptography
PKI	public-key infrastructure
PQC	post-quantum cryptography
QIC	Quantum Industry Canada
QKD	quantum key distribution
QRC	quantum-resistant cryptography
QSC	quantum-safe cryptography
RSA	Rivest-Shamir-Adleman
SMEs	small and medium-sized enterprises
SNDL	store now, decrypt later
SSH	secure shell
TBS	Treasury Board Secretariat
The Cyber Centre	Canadian Centre for Cybersecurity
TLS	Transport Layer Security
VPNs	virtual private networks

Executive Summary

The rapid advancement of technology continues to drive innovation across sectors such as finance, health care, defence and telecommunications. However, these developments also introduce new risks, particularly with emerging dual-use technologies such as quantum computing. While quantum computing presents transformative opportunities, it also threatens current cryptographic systems, rendering them vulnerable to attacks that could compromise sensitive data across both the public and private sectors. This special report acknowledges these challenges and affirms the critical role of government in steering regulatory development. It is intended for policy leaders and other actors concerned with cybersecurity.

Post-quantum cryptography (PQC) is a key safeguard in a multi-pronged strategy to build long-term security by strengthening digital infrastructure resilience. However, the transition to PQC must occur proactively before cryptographically relevant quantum computers (CRQCs) can break current encryption standards. The recent release of PQC standards from the National Institute of Standards and Technology (NIST) represents a significant milestone in this transition, but major challenges remain, particularly in establishing an effective strategy for PQC adoption across Canada's public and private sectors.

Despite ongoing research into the technical and policy aspects of PQC, questions persist regarding the governance and regulation of PQC implementation in Canada. Should the transition be led by the public sector through government-mandated regulations, or can private sector adoption be sufficiently managed through market incentives? This special report assesses Canada's approach to PQC migration by comparing regulatory frameworks, public-private collaboration and sector-specific strategies to inform policy.

While both public and private actors have important roles to play, expert interviews and literature reviewed throughout this special report reveal that without government leadership, migration will be delayed by market hesitation, uneven readiness across sectors and insufficient coordination. Given the risks to national security, critical infrastructure and public trust, a government-led approach is essential to ensure timely, equitable and interoperable adoption of quantum-safe standards.

To facilitate a secure and efficient transition, the special report outlines a series of key policy recommendations.

A Call for Early Action on PQC Migration

Addressing the urgency: Threat actors can already store encrypted data, with the intention of decrypting it once quantum computers reach the necessary capabilities. This underscores the urgent need to transition to PQC before CRQCs become viable.

Identifying early adopters: Regulatory bodies should identify and prioritize critical sectors for PQC adoption, including finance, health care, energy, defence and government infrastructure. A phased, risk-based migration strategy should be implemented, beginning with high-priority sectors and expanding gradually.

Risk-based prioritization for migration: Organizations must conduct comprehensive cryptographic inventories to assess vulnerabilities and prioritize migration based on risk exposure.

Stimulating the Adoption of PQC

Financial and resource support: Governments should provide targeted financial support by leveraging national quantum strategies, and through tax credits and grants to help organizations manage PQC transition costs.

Building public-private partnerships: Collaboration between government, academia and industry is essential to overcoming barriers such as high switching costs and a lack of technical expertise.

Education and training initiatives: Centralized resource hubs and educational programs can support organizations in navigating the complexities of PQC migration. Investing in education initiatives for industry leaders and smaller organizations, alongside training the next generation of cryptographic professionals, is essential to overcome financial and resource constraints.

Ensuring equity in adoption: To prevent tiered access to cryptographic protections, public support should prioritize small and medium-sized enterprises (SMEs), non-profits and public institutions with limited cybersecurity capacity. PQC migration strategies must be designed to promote equitable access across sectors.

Public communication and misinformation management: A national communication campaign should be developed to proactively address public misconceptions and build trust in PQC technologies, mitigating the risk of misinformation-driven backlash as seen in other emerging-tech domains.

Leveraging market incentives and procurement standards: Governments should incorporate PQC readiness into procurement requirements, using public sector purchasing power to drive adoption and normalize PQC across industries.

Government-Led Initiatives

Regulatory measures and international cooperation: Canada should leverage its regulatory framework to align PQC adoption with its key trading partners, ensuring interoperability across global standards. Establishing formalized standards and certification processes will provide industries with clear guidelines for transitioning to PQC. Additionally, Canada should prioritize setting regulations with clear migration deadlines for sectors handling sensitive data to ensure timely and effective security measures.

Reassessing national strategies: National quantum strategies should be viewed as starting points rather than endpoints, requiring regular reassessment to address emerging applications. The strategy should adapt to evolving quantum risks and include interdisciplinary expertise to bridge technical challenges with policy making.

Diversifying international engagement: To reduce reliance on any single jurisdiction, Canada should strengthen its regulatory and standardization ties with multilateral bodies such as the European Union and the European Telecommunications Standards Institute (ETSI), ensuring resilience through global interoperability.

Canada's role in global quantum-safe standards: Canada should lead regular policy-maker meetings and informal consultations to ensure international alignment on quantum-safe transitions.

Failure to take urgent action may expose Canada's digital infrastructure to significant risks. Canada has an opportunity to lead in quantum security. Adopting a proactive policy approach that emphasizes outcome-focused regulation — by setting clear transition timelines and leveraging market forces — can position Canada at the forefront of PQC adoption while also safeguarding national security in the quantum era.

Introduction

Quantum computers are a novel technology grounded in quantum mechanics — notably, superposition and entanglement — that enable fundamentally different modes of information processing than classical computing, with the potential to accelerate solutions to complex problems and revolutionize many industries. At the same time, quantum computing poses a significant risk to current cryptographic systems that safeguard sensitive data and communications across industries and governments.

Public-key cryptography (PKC), a system introduced in 1976, has been the backbone of secure digital communications. It facilitates the secure exchange of information without the need for a pre-established private connection between the parties involved. This set of cryptographic methods relies on mathematical problems that are virtually impossible for today's computers to solve. However, quantum computers can solve some of these problems much faster, rendering current cryptographic algorithms, such as Rivest-Shamir-Adleman (RSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA), ineffective (Chen and Scholl 2022).

Replacing outdated public-key algorithms is necessary regardless of the timeline for quantum computing advancements. Algorithms such as RSA and ECDSA, which currently protect all internet traffic, are vulnerable to quantum attacks and must eventually be replaced to maintain security as quantum computing progresses. While these algorithms are regularly updated by increasing their key sizes to remain secure against classical computers, quantum computers can compromise them regardless of key length (Campagna et al. 2015).

A recent Google Quantum AI study finds that a quantum computer with about one million noisy qubits could break the widely used RSA-2048 cryptographic algorithm in roughly one week (Gidney 2025). This is a 20-fold drop in hardware requirements compared with Google's estimates from 2019. Although today's quantum computers are only hundreds to a few thousands of qubits (ibid.), this sharp reduction in the resources needed highlights the urgency of securing critical data against the quantum threat.

The emergence of quantum computers raises an urgent need to transition to new cryptographic systems designed to resist quantum-based attacks. These systems, known as PQC, are being developed to protect sensitive information in a world with quantum computers. Without such measures, critical sectors such as health care, finance and infrastructure are vulnerable.

Quantum key distribution (QKD), which is based on the principles of quantum mechanics, is also viewed as a promising defence, yet given current technical hurdles, its practical deployment remains limited for now (Innovation, Science and Economic Development Canada [ISED] 2025). Accordingly, this special report concentrates on the more immediately scalable path of PQC.

One of the severe risks includes the possibility of "store now, decrypt later" (SNDL) attacks. In these scenarios, threat actors collect encrypted data, with the intention of decrypting it once quantum computers become available. This would expose sensitive information and jeopardize data security and trust (De Luca 2024).

A key parameter when evaluating SNDL risk is the shelf life of data, defined as the length of time the information must remain confidential. Data that must stay secret for decades, such as health records, presents a higher SNDL risk (Mosca and Piani 2021).

Quantum computing promises benefits such as advancing financial modelling, accelerating drug discovery and enhancing artificial intelligence (AI). However, these opportunities also come with risks (Deodoro et al. 2021). By acting now to adopt PQC, policy makers and organizations can protect the systems and data that underpin the modern digital economy, ensuring that the promise of quantum computing does not come at the expense of security and trust.

Although ongoing research addresses the technical aspects and policy perspectives of PQC, further investigation is needed into how PQC should be governed and regulated — specifically, whether it should be managed by the public sector or led by the private sector in Canada. This special report provides critical insights into effective governance and regulatory approaches for PQC, to ensure the security of Canada's digital infrastructure against quantum threats. By assessing regulatory and market-driven initiatives, this research aims to safeguard digital communication in Canada through a secure and efficient transition to PQC.

Drawing on a comprehensive analysis of existing research on PQC, the authors examine the strategies currently pursued by public and private sector actors in Canada, with particular attention to standardization initiatives. As detailed in Table 1, the authors conducted interviews with anonymized PQC experts across public, private and academic sectors.[1] Building on these findings, the authors propose a set of policy insights and recommendations aimed at supporting a secure and effective transition to PQC.

This special report is structured as follows. The section "Risks of the Quantum Threat" introduces the quantum threat to public-key infrastructure (PKI) and the necessity of migrating to PQC. "Deployment Challenges" highlights the obstacles organizations will face both in preparation for and during migration, divided by technical, organizational and governance-related issues. "Incentive and Market Forces" explores incentives for leading the adoption of PQC, emphasizing the market's role as both a catalyst and a driving force for its implementation. "Standards, Certification and Regulation" outlines the processes involved in regulating cryptography, highlighting how regulation can support PQC adoption. This includes the standardization of PQC, the current regulatory landscape and potential methods for governing migration. "Varying Regulatory Frameworks" examines regulatory approaches across jurisdictions, focusing on Canada and its cryptography regulatory bodies, the United States and the European Union, while highlighting factors shaping these approaches. "Evaluation of Public-Private Sector Roles in Canada" evaluates the roles and initiatives of the public and private sectors in driving PQC adoption, both independently and collaboratively. Finally, the conclusion summarizes key findings and policy recommendations, followed by appendices describing the authors' research approach and additional information on topics discussed earlier in the special report.

1 To encourage candid responses, the authors assigned pseudonyms to each interviewee and altered any details that could reveal their identity.

Table 1: Interview Participants, by Occupational Role and Sector

Pseudonym	Expertise/Occupational Role	Sector
PR1	Quantum-safe cryptography (QSC) schemes	Private
PR2	Cybersecurity and PQC as a co-founder of a cybersecurity company	Private
PR3	Former chief information officer (CIO)	Private
PR4	Wireless and emerging technology, and global standards	Private
PR5	Cybersecurity executive specializing in quantum-safe security solutions	Private
PR6	Quantum-computing company executive	Private
PR7	Research scientist focusing on QKD	Private
PR8	Quantum-cryptography company executive	Private
PU1	Standardization governance and quantum and technology policy	Public
PU2	Regulations and policies surrounding cryptography and cybersecurity in Canada	Public
PU3	Quantum scientist in the financial services sector	Public
PU4	Quantum computing scientist	Public
PU5	PQC standardization in the United States	Public
PU6	Quantum software engineer	Public
A1	Information technology (IT) management and quantum-resistant solutions	Academia
A2	PQC and its societal impact	Academia
A3	Legal implications of technology	Academia
A4	Cryptography	Academia
A5	Technology governance	Academia

Source: Authors.

Risks of the Quantum Threat

In this section, the authors first outline migration timelines, with consideration for the technology life cycle. Next, the authors address the risks of quantum threats to critical infrastructure and operational technology (OT), such as in the energy sector. Finally, the authors examine the societal impact, highlighting how this threat could affect civilians.

For organizations in the public and private sectors alike that rely on secure information, the consequences of not transitioning to PQC may be catastrophic, impacting critical infrastructure, financial institutions and health-care organizations. This could lead to severe impacts on civilian data and, in extreme cases, result in loss of life.

The concern stems from the fact that most technologies currently in use rely on cryptographic schemes that are not quantum-safe, making them susceptible to quantum-enabled attacks. While we do not yet have CRQCs, their development could undermine the security of systems built over the past several years.

Risk Timelines and Technology Life Cycle

PR1, a private sector expert in QSC, highlighted the risks of delaying the transition of critical infrastructure to quantum-resistant cryptography (QRC). For example, energy plants may require 10–15 years to implement and standardize such changes. Given NIST's target of being quantum safe by 2035, delaying transition efforts could push readiness to the mid-2040s — by which point it may be too late to respond effectively to emerging threats. The PQC transition requires addressing both the technical modifications to energy systems and organizational processes, such as approvals, that can further extend timelines set for transitioning.

In addition to these timelines, consideration must be given to the life cycle of hardware. Satellite systems, for example, cannot be retrieved once launched, it is therefore crucial to consider their encryption technology. A satellite launched today without QSC could remain in orbit for 10–20 years, when CRQCs may already exist. Experts highlighted the potential impact of the quantum threat on everyday systems and OTs that civilians rely on. And as the authors will further describe, these experts also outlined how hacking OT and critical infrastructure — such as satellite systems, cars, water supplies or elevators — could result in severe consequences, including loss of life.

Building on the earlier example about satellites, PR2 explained that these risks involve challenges we have not faced before. PR2 noted that "going forward, if your car gets hacked, if the water supply gets hacked, if the elevators you're in get hacked, or if the satellite communication system that you need gets hacked, the consequences are different....Many of these systems...have a much more radical impact on human lives — you know, a very potential threat to human lives."

Illustrative Quantum Threat Scenarios for Critical Infrastructure and OT

Quantum threats to OT demand careful consideration. A1, a specialist in IT management and quantum-resistant solutions, noted that "operational technologies are completely different beasts" when comparing the IT migration process to that of OT. Presently, experts and organizations concentrate their migration efforts on IT systems. For example, financial institutions are prioritizing the shift to PQC for their IT cryptographic schemes. Nevertheless, OT and critical infrastructure systems, such as those employed in the energy and oil and gas sectors, also require substantial attention.[2] Experts raised several examples of risks to critical infrastructure and OT:

- PR3, a former CIO for several Fortune 500 companies, highlighted the risks to air traffic control systems, describing the catastrophic consequences of a threat actor using a quantum computer to hack the operational control centre software guiding planes, or the software aboard the plane itself.
- PR2 emphasized the importance of securing OTs in smart cities, smart cars and smart homes, where a key challenge is maintaining long-term security. For example, a smart car with firmware update capabilities purchased today could become vulnerable within 10–20 years as quantum computers develop. This vulnerability could enable threat actors to hack and control automated driving software.
- The stakes in the energy sector are particularly high, as a quantum-enabled attacker could cause widespread blackouts. The implications of extended blackouts in metropolitan cities across Canada would be severe, jeopardizing civilian livelihoods and critical systems that rely on electricity.
- Electric power grids are reliant on real-time data, advanced sensing and wireless communication networks due to their interconnected nature. This introduces new vulnerabilities, increasing the risk of cyberattacks aimed at disrupting energy infrastructure, such as the 2015 Ukrainian power grid hack. A quantum-enabled attacker could exploit these weaknesses by breaking cryptographic schemes that secure information transfer, allowing manipulation of critical infrastructure controls and causing large-scale power outages.
- The electricity sector is particularly at risk due to the interconnectedness of distributed energy resources, grid-control systems and Internet of Things (IoT) devices. If quantum computing is leveraged to break cryptography securing these systems, attackers could compromise the resiliency of electric power networks, posing a threat to infrastructure stability.
- One example of the risks posed by the quantum threat to the interconnected electricity sector is if internet-connected household devices, such as smart fridges and smart meters, were remotely turned off for millions of residents simultaneously by a threat actor. This could create an imbalance in grid frequency, where the electricity consumed and generated causes fluctuations. Such large and sudden changes in frequency can damage infrastructure and

2 While IT refers to systems and equipment, such as software used to manage and process data, OT encompasses systems and devices that monitor, manage and control real-world processes and events, commonly found in industrial automation, building management, fire safety and access-control systems. See NIST (2023); Vermeer et al. (2023).

trigger power outages (Denholm et al. 2020). Beyond disrupting electricity distribution, this specific scenario could also lead to food spoilage and economic losses. These seemingly harmless IoT devices in homes can serve as entry points for cyberattacks that have the potential to destabilize the entire power grid (Ratnam et al. 2020).

- The vulnerability extends beyond financial institutions to critical infrastructure. Experts outlined a scenario in which a quantum-enabled attack could target the Ministry of Infrastructure and Water Management in the Netherlands, causing flooding. Such attacks could also be exploited for ransom, with devastating consequences for citizens.

- In extreme cases, quantum-enabled attacks breaching cybersecurity systems could lead to public panic and civil unrest if not addressed promptly. A2, an expert on PQC and its societal impact, cited the Netherlands' ABN AMRO bank as an example, noting that while some chief information security officers (CISOs) recognize the quantum threat, they prioritize immediate concerns such as zero-day attacks. This short-term focus risks larger-scale consequences, according to A2: "If they don't migrate now…it will be the people or citizens at the end of the day who will be badly affected." They warned that failure to migrate could lead to financial system collapses, automated teller machine (ATM) outages and widespread panic.

A report from the Hudson Institute warns that a quantum-enabled cyberattack on financial infrastructure could trigger cascading failures worse than the 2008 global financial crisis or even the Great Depression, as the interconnectedness of banks means an initial breach can rapidly spread systemic risk across global markets (Herman and Butler 2023). European scenario analyses from the Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations project caution that compromising financial-sector cryptography could lead to the collapse of the global banking system, causing national economies to fall and potentially breaking down the international financial order. The societal consequences could be severe: If online banking and digital payments were disrupted, panic-induced bank runs, ATM outages and cash shortages could escalate into civil unrest, with violence and intimidation erupting as people compete for scarce resources (Meijaard, Spagnuelo and Bharosa 2023).

Civilian Impact and Public Perception

Public perception and trust are essential in addressing quantum threats and integrating quantum technology into sectors such as finance and critical infrastructure. A3, an expert on the legal implications of technology, highlighted the risks of misinformation and public panic, drawing parallels to the backlash against fifth-generation (5G) technology. They cited incidents of "people burning down 5G radio towers" to illustrate how fear and mistrust can hinder technological progress. Similarly, misinterpretations and misrepresentations of quantum advancements in the media could create resistance to adopting the technology. For instance, when Samsung announced its phones were equipped with a quantum random number generator chip, misleading headlines such as "quantum phones are here" created misconceptions about what "quantum-safe" truly means.

These challenges are exacerbated by the urgent need to protect military and government data from quantum-driven threats. Securing this information involves determining who can use quantum computers and identifying which data they might

seek. Experts caution that states with quantum capabilities could launch attacks on others, highlighting the critical importance of fortifying sensitive government resources.

Deployment Challenges

This section examines the challenges in adopting PQC across three dimensions: technical, organizational and regulatory. It addresses technical challenges in integrating PQC with existing systems and examines which algorithms are best suited for adoption. Organizational challenges include varying levels of awareness across sectors about the quantum threat, communication barriers, the need to balance urgency with transition timelines, and resource constraints in talent and finance. Lastly, the section highlights regulatory obstacles, the impact of geopolitical dynamics on standardization, and the importance of prioritizing initiatives for PQC migration alongside other emerging quantum technologies.

A key technical hurdle for organizations is the lack of awareness about the components of existing cryptographic systems. This is especially problematic in legacy infrastructure, where outdated systems with long lifespans are vulnerable to quantum threats. Technical issues are amplified by organizational challenges, including inconsistent awareness levels, talent shortages, financial constraints, communication gaps between technical experts and policy makers, and the need to balance immediate and long-term cybersecurity priorities. Additionally, questions remain about which sectors should act as early adopters. Geopolitical dynamics further complicate these decisions, highlighting the importance of interoperability and the need for dedicated funding and resources to support the PQC migration process.

Technical Challenges

Migrating to PQC and addressing vulnerabilities in cryptographic systems is complex due to the challenges organizations face in preparing for and managing the transition. This process includes managing root certificates, conducting crypto inventories, updating legacy systems, and the unpredictability surrounding evolving standards and technologies. These issues highlight the need for flexible and proactive approaches to ensure a secure transition.

Implementing PQC comes with deployment challenges, some of which are unknown, largely due to the complexity of existing systems and the lack of a clear transition process. A major hurdle is identifying and documenting the cryptographic schemes already in use. PU2 pointed out that the challenge lies in the long life cycle of certain hardware, such as network routers and edge devices, which may stay in operation for decades without being updated to meet new cryptographic standards. Managing these large, complex networks adds another layer of difficulty because it is hard for system owners to track their equipment, locations and cryptographic algorithms. A2 reinforced this point, pointing out the necessity of having a cryptographic inventory as the first step. They emphasized the importance of first understanding all system components in order to develop an immediate action plan. This underscores the need for organizations to map and update their systems to ensure a smooth transition to PQC.

Root Certificates

Root certificates are public-key certificates issued by a trusted certificate authority. They enable secure communications by establishing trust between parties, such as websites and browsers, ensuring data integrity and identity verification. The public nature of root certificates makes them particularly vulnerable in a post-quantum world, where quantum computers could break cryptographic algorithms. PR5, a CEO of a cybersecurity company specializing in quantum-safe solutions, emphasized the difficulty of managing and prioritizing root certificates due to a limited understanding of which certificates are actively in use. In addition, compromising a single root certificate could have major consequences; solving one mathematical problem using a CRQC, such as a discrete logarithm or factoring problem, could enable attackers to breach an entire system's security, impacting both public and private sectors that depend on these systems for secure communications and data protection.

Root certificates often have a lifespan of up to 30 years, posing a long-term security risk. Even with a CRQC, these certificates would remain in use, leaving systems vulnerable. The extended lifespan of root certificates therefore further complicates the issue, as many organizations are unprepared for large-scale PKI migrations or the unexpected challenges they may face during the process.

Crypto Inventory

According to experts PR1 and PU3, implementing PQC will be challenging for organizations because many lack a complete inventory of their cryptographic systems. Without this inventory, transitioning to PQC becomes complex, as a vulnerability down the supply chain would require organizations to uproot their entire cryptographic infrastructure. A key first step in migrating to PQC is for organizations to develop a "crypto inventory," a comprehensive understanding of the cryptography currently in use. PU5, who helps develop PQC standards for the US government, explained that many organizations do not understand which data they are encrypting, how it is encrypted, or why. They also struggle to track basic details, including the certificates in use, their providers and the lifespan of machine secure shell (SSH) certifications.

Internal vulnerabilities further complicate the transition. PR5 noted that while external interfaces are often secure, internal systems remain exposed. Companies often prioritize securing external entry points such as firewalls, virtual private networks (VPNs) and web-facing applications since they are the most visible and commonly targeted by external attackers. However, internal systems are frequently neglected, leaving vulnerabilities such as unencrypted emails and traffic exposed, which PR5 described as "completely visible." These internal weaknesses are particularly dangerous because attackers, whether external hackers or insiders, can exploit these blind spots once they gain access. The problem is exacerbated by what PR5 described as the "organically grown" nature of internal systems, where they are developed over time in an unstructured manner without a cohesive or organized approach, making them difficult to track and secure effectively. Additionally, many organizations are unaware of these vulnerabilities, further increasing the risk of insider attacks.

Managing large, complex networks presents added challenges. However, with a clear understanding of their systems, organizations can prioritize urgent tasks and position themselves for a smoother transition to PQC.

Crypto Agility and Legacy Systems

To develop a comprehensive inventory of their cryptographic assets, organizations must begin by documenting all existing cryptographic systems. As PU2 noted, components such as network routers and edge devices can remain in operation for decades without being updated to support new cryptographic standards, resulting in long-term vulnerabilities. Building this inventory is a critical step toward achieving crypto agility — the ability to quickly adapt systems to evolving cryptographic requirements — which experts emphasize as crucial for transitioning to PQC.

Legacy systems pose a major challenge to adopting PQC, especially in government and defence. PU5 explained that in the United States, many government systems are outdated, custom-built and difficult to update or upgrade. These systems often operate continuously at scale, making it impractical to shut them down for updates. Given their integration into critical infrastructure, implementing large-scale updates without disrupting operations is a significant obstacle.

Experts highlighted that while crypto agility is essential for easing the transition, it can pose challenges in high-security sectors, where systems are often designed to be locked down and difficult to modify. Transitioning to a crypto-agile system, such as swapping algorithms, can create temporary vulnerabilities. For example, in the Netherlands' Ministry of Defence, systems become briefly exposed during transitions, increasing the risk of breaches. In high-security settings, even a slight reduction in security — being 99 percent secure instead of 100 percent — is deemed unacceptable, complicating these transitions.

The push for crypto agility is especially urgent, given uncertainties about the long-term viability of newly adopted algorithms. A2 cautioned against protocol ossification, where outdated systems become so entrenched they are nearly impossible to update or replace. A3 emphasized that achieving crypto agility represents a significant shift in cybersecurity practices and will require a large-scale, industry-wide effort. PR1 emphasized that transitioning to PQC not only strengthens existing cryptographic systems but also diversifies the algorithms used, reducing the risk of sudden failures caused by either quantum or classical threats.

Organizational

In addition to the technical challenges of preparing and maintaining systems for migration to PQC, there are significant organizational challenges. Experts identified inconsistent awareness levels across sectors as a major barrier to readiness, with some industries more prepared for quantum threats than others. Another key challenge is balancing immediate cybersecurity risks with long-term quantum computing threats.

Experts also highlighted difficulties in communicating the technical complexities of PQC migration to non-technical decision makers, which can delay decision making and resource allocation. Further challenges include a shortage of skilled personnel and the financial constraints many organizations face when planning large-scale transitions. Given the complexity of migration, there are ongoing discussions about which sectors should act as early adopters and when PQC adoption should begin.

Public-Private Awareness

A significant challenge in advancing PQC is the differing perspectives among stakeholders about the urgency of transitioning. Experts highlighted the need to convince industry executives, many of whom see CRQCs as a distant issue and

are reluctant to invest in a quantum-safe transition now. In addition, people often underestimate the time needed for the transition to PQC and overestimate how long it will take for CRQCs to materialize. They stressed that efforts to improve Shor's algorithm[3] are accelerating quantum computing advancements, shrinking the preparation window in ways many fail to grasp.

A1 reasoned that organizations should not wait for the arrival of CRQCs to start preparing. They compare cybersecurity to fire insurance: Even if there is no immediate timeline for a fire, people insure their homes to protect against potential risks. Similarly, organizations should secure current cryptographic systems now, as the overall risk of CRQC increases with its potentially significant impact. The concern is not only the emergence of CRQCs themselves but also the period beforehand, when sensitive data can be intercepted and stored for future decryption. This SNDL threat highlights the urgency of proactive cryptographic protection, especially for data with long-term confidentiality needs. To measure urgency, the authors applied Mosca's $x + y > z$ model: If the data's shelf life (x) plus the time required to migrate to PQC (y) is greater than the expected timeline for a cryptographically relevant quantum computer (z), confidentiality cannot be assured (Mosca and Piani 2019; Mosca and Mulholland 2017).

Further, while CRQCs are typically treated as an exogenous threat, some experts argue that widespread PQC adoption may itself shape the pace of quantum development, potentially reducing incentives to develop cryptanalytically useful quantum computers. This suggests that proactive migration could not only mitigate future risk but also influence its trajectory. Risk assessment thus plays a key role in addressing quantum threats, involving an evaluation of both the likelihood and potential impact of quantum-enabled attacks.

There is also debate about the likelihood of quantum computers becoming a threat. Within academia, cryptography experts hold differing views on the level of urgency, leading to a fragmented message for industry stakeholders. This inconsistency extends to the public and private sectors, where readiness and expertise vary significantly. For example, while organizations such as the Canadian Security Intelligence Service are advancing in transitioning to PQC, other government departments lag in preparedness and expertise.

A4 explained that the private sector's readiness for PQC adoption is mixed, depending on organizational resources and size. Financial services and technology firms are generally aware of the upcoming changes and are already taking steps to prepare. These organizations typically have dedicated cybersecurity teams, including cryptographers, who closely monitor emerging technologies and know what the regulatory requirements look like. Many of these companies have likely already conducted experiments with PQC, worked with vendors to test prototypes and evaluated how these solutions integrate with their existing infrastructure.

Competing Narratives and Priorities

A recurring theme in discussions about the quantum threat is the competing priorities among stakeholders. Experts noted a tension between addressing

3 Shor's algorithm, created by mathematician Peter Shor, is a quantum algorithm that can break down large composite numbers into their prime factors far more rapidly than any known classical method, achieving an exponential speed-up. Since modern cryptographic algorithms such as RSA rely on the difficulty of factoring, this breakthrough carries major implications for cryptography. See www.quera.com/glossary/shors-algorithm.

immediate operational challenges and planning long-term strategies for emerging technologies such as quantum computing. This dynamic is seen in organizations through the way they allocate resources, prioritize investments and perceive the urgency of specific challenges among different stakeholders. The difficulty lies in balancing an organization's current needs with proactive measures to address future quantum threats, such as adopting PQC.

PR3 illustrated this dynamic by discussing the responsibilities of CIOs. In the context of the airline industry, they explained that CIOs prioritize current security needs, such as designing network architectures to ensure operational safety, over distant concerns such as potential breaches by quantum computers. This operational focus often leaves little room for integrating solutions such as PQC into corporate cybersecurity plans. There is also the issue of corporate investment in PQC; CISOs, who typically serve for only three–five years, are unlikely to prioritize long-term risks that may not materialize during their tenure.

The focus on immediate priorities rather than long-term risks is complicated by legal and financial concerns. CISOs may fear lawsuits for negligence if they do not address known risks, but they might hesitate to invest in PQC due to the lack of immediate financial benefits. Because the business implications of PQC adoption are unclear, it is hard to justify investment. Some experts cautioned that advancements in quantum computing should serve as a catalyst for raising awareness and motivating stakeholders to take PQC more seriously. These perspectives illustrate the competing narratives driving organizational responses to the quantum threat. Industry leaders often believe that quantum computers are too far in the future to prioritize now, contrasting with the view that rapid advancements in quantum computing should drive early planning for the transition to PQC. From a corporate cybersecurity leader's standpoint, pressing operational needs tend to overshadow investments in PQC, especially when there are no clear financial incentives to justify prioritizing long-term security measures.

Communication Barriers

Technical explanations of the quantum threat often fail to convey its urgency to non-technical audiences. For instance, researchers might present 15-year timelines for the emergence of quantum computers, but decision makers are likely to be swayed by a more urgent message, such as "you are already too late."

A2 emphasized that communication barriers exist at every level, making it hard for experts to effectively convey the seriousness of quantum-related issues. When asked how to communicate such complex issues effectively to policy makers and industry leaders, A2 pointed to the importance of having compelling speakers. They shared an example of a colleague at a small quantum-technology start-up in the Netherlands who is highly effective at bridging this gap. This individual, who combines deep technical expertise with industry experience, delivers messages in a way that resonates with their audience, making policy makers and industry leaders more likely to take the issue seriously. A2 noted that biases, such as the speaker's authority and presence, play a role in how the message is received. They reflected on how their own younger age, shorter stature and gender might make their message less impactful, even if it is equally accurate and well delivered.

Urgency and Timelines

Balancing the urgency of addressing security risks posed by the quantum threat with the practical timelines for implementing PQC is challenging for many organizations. A2 noted that while some companies are indifferent to the security risks, even those that do care face lengthy transitions. This is due to the need to fully understand their systems and available solutions, which are only now emerging as part of the NIST standardization process.

Some experts believe regulation can play a crucial role in establishing timelines for transitioning to PQC. They point to the United States as an example, where companies handling certain types of government data are required to complete their migration by 2035 (Cybersecurity and Infrastructure Security Agency [CISA] 2024). PR1 shared an example from Germany's standardization body, the *Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for Information Security, or BSI), which aims to migrate its systems to PQC by 2030. However, when asked about the starting point for this migration, the BSI did not specify a date.

PR8, the CEO of a PQC company, stressed the urgency of starting transitions immediately. They noted that while some advocate for an upgrade of global cryptographic systems, the reality is more complicated. In places such as the Netherlands, large-scale projects for organizations often face delays and resource constraints, extending timelines far beyond initial estimates. The conflict between balancing urgency with practical limitations without compromising quality makes efforts to meet PQC standards difficult.

Resource Constraints

A major issue in implementing PQC is allocating the necessary resources, as many organizations lack both the personnel and financial backing to execute the migration effectively. For example, banks recognize the need to address PQC but face hurdles such as limited education, talent and expertise in quantum technologies. Bridging this gap requires upskilling employees and investing in skills training. Securing corporate investment in PQC is another obstacle; although it is understood that NIST-approved algorithms will require more memory and computing power, the precise costs of necessary hardware investments are unknown. This stands in tension with decision makers' need for clear timelines and cost estimates. Without concrete answers to questions about when the transition will occur or how much it will cost, decision makers often lose interest before meaningful progress is made.

PR8 emphasized the global shortage of skilled workers required for PQC implementation, pointing out that there are few professionals who can properly administer the necessary protocols, and this shortage is only worsening. These constraints highlight the need for targeted training programs and increased funding to prepare for a quantum-safe future.

Deploying PQC requires investment in talent and resources to secure the future of cryptographic systems in addition to addressing the technical challenges. PR2 highlighted a critical talent gap in cryptography, stemming from decades of inaction. Over the past 30 years, too few bright minds have been encouraged to pursue careers in cryptography, with many instead gravitating toward fields such as quantum computing, AI and cloud computing. As a result, the pool of cryptography experts is shrinking, with many nearing retirement, just as challenges in the field are expanding.

First-Mover Benefits and Drawbacks

A key concern in transitioning to PQC is timing, as standards are still in development. While companies such as Apple and Google have begun integrating PQC, being a first mover introduces risks. PR6, a quantum computing CEO, stressed the need for flexibility and urgency in navigating evolving standards. Start-ups, governments and corporations must act quickly to address long-term security challenges, particularly the protection of sensitive, long-lived data. However, PR6 cautioned against premature decisions that risk adopting non-standardized algorithms, potentially wasting resources. They emphasized a balanced approach — staying proactive while avoiding ineffective or harmful choices. It is important that start-ups follow standards to ensure that PQC implementations are standardized and meet evolving security needs. By starting to implement PQC, organizations can minimize vulnerabilities and prepare for future risks.

A few key stakeholders responsible for specific data security functions will largely determine how quickly and safely others can migrate. Pinpointing these critical functions is therefore essential. National Critical Functions (NCFs) are the 55 essential activities identified by the US Department of Homeland Security that underpin national security, the economy and public health, spanning everything from internet services to electricity distribution. These functions are delivered by a mix of public and private sector providers. A 2022 RAND report stresses that although fully eliminating quantum-related risks will require nearly every NCF to adopt PQC, upgrading three key NCFs first would rapidly reduce much of the current risk (Vermeer, Parker and Kochhar 2022).

These three functions supply the hardware, software and trust services on which all other critical sectors depend. NCF 3 covers cloud platforms, web-hosting providers, and other internet-based services that move and store data online. NCF 35 covers certificate authorities and identity-management firms that issue and manage the digital certificates used online. NCF 52 includes the IT vendors whose hardware and software embed cryptographic tools. Together, NCFs 3 and 52 manage the cryptography that protects data, while NCF 35 supplies the digital certificates that verify online identities. Until they provide quantum-resistant versions of these tools, such as updated web-encryption protocols, VPNs and digital certificates, other sectors cannot complete their own transitions, and older, more vulnerable systems will stay in use (ibid.).

The lack of regulation in some sectors complicates adoption. A1 noted that federally regulated industries, such as critical infrastructure, are making progress while non-regulated sectors, such as health care, lag. A domino effect is expected: Vendors improving cybersecurity to meet strict federal requirements will indirectly benefit non-regulated customers by offering enhanced security measures. However, these benefits may be delayed as changes gradually trickle down through the system.

Experts debate whether the public or private sector should lead PQC adoption. A2 argued that private companies are better positioned to navigate implementation failures without affecting sectors critical to public welfare, unlike public sector organizations such as hospitals or critical infrastructure providers. PU6, a quantum software engineer with the Government of Canada, argued that the public sector is better suited to lead the PQC migration. They noted that governments face less financial risk than private companies and can benefit from research conducted during the process. Additionally, public trust in government, positioned between academia and industry, could be leveraged to drive a successful migration.

Community-Driven Efforts

A2 emphasized that community-driven initiatives play a pivotal role in testing and advancing the adoption of PQC. Open-source communities, often led by enthusiastic engineers, are instrumental in developing early implementations — such as Python tools — that showcase how new cryptographic methods can be integrated and scaled. By actively creating solutions for high-demand languages such as Go, Java and Python, these communities help lower barriers to entry for organizations of all sizes. Their collaborative work ensures that developers can quickly implement and test PQC algorithms, ultimately accelerating the broader transition to PQC across the tech ecosystem.

Regulatory

The focus on short-term quantum applications often sidelines critical areas such as PQC. Experts warn that prioritizing immediate benefits, such as quantum computing and sensors, leads to underfunding PQC, despite its importance for long-term cybersecurity. Tackling this issue requires international collaboration, strategic investment and a balanced approach to support the interconnected quantum technology landscape. This approach includes acknowledgng the role of geopolitical dynamics in shaping the adoption and deployment of PQC.

Geopolitical Dynamics and the Impact on Standardization

Political and economic relationships shape the adoption of regulatory frameworks, particularly in areas such as PQC. A5 pointed out that while standardization — for instance, by NIST — can play a crucial role in mitigating security threats, the decision to align with one set of standards over another is ultimately driven by broader political and economic considerations. Countries often opt for standards that support their strategic supply chain interests, whether in military, transportation or other vital sectors.

Historically, Canada's strong economic and security ties with the United States have led it to favour US-aligned standards — a trend reinforced by its participation in alliances such as the Five Eyes, which also includes Australia, New Zealand, the United Kingdom and the United States. PU4 noted that the global prominence of American technology, exemplified by Microsoft's Windows operating system integrating NIST-aligned cryptographic software, underlines the importance of international cooperation in establishing widely adopted standards. Recently, there has been increased work on the transition to PQC in the European Union, marked by a newly released adoption road map, and this coincides with emerging signals of closer collaboration between Canada and the European Union. In this evolving geopolitical landscape, these factors suggest that while past alignments have favoured US-centric frameworks, Canada may continue to reassess its strategic partnerships and standardization choices as global dynamics shift.

Siloing of Quantum Technology Investments

Funding often prioritizes quantum technologies with near-term applications, overlooking critical areas such as PQC. A5, a technology governance researcher, notes that this short-term focus can lead to siloed decision making. Advancing PQC, however, requires stronger integration with other quantum fields — particularly quantum computing — to avoid confining its development under quantum communications. As quantum computing progresses, the urgency of implementing

PQC grows, yet efforts still risk becoming siloed if organizations remain narrowly focused on immediate gains. While quantum computing warrants continued investment and collaboration, recognizing and cultivating ties among all quantum technologies is essential to ensure PQC receives the attention it demands within the broader ecosystem.

The short-term focus with investing in quantum technologies leads to underfunding and overlooking solutions such as PQC, which are crucial for mitigating long-term threats. In actuality, PR6 and others argue that PQC is more closely related to security than to computing, and grouping it under broader categories such as quantum communication often diminishes its importance.

Moreover, national strategy documents, such as the National Quantum Strategy (NQS) (ISED 2022), should explicitly highlight the quantum threat and strengthen the connection between quantum computing developments and the urgency of PQC migration. This can be achieved by setting distinct investment areas with clear challenges and milestones for PQC adoption. This approach can help highlight and address the threat of SNDL attacks, ensuring that sensitive data remains secure with the development of quantum computing.

Additionally, A5 noted that the divide between public and private sector actors exacerbates silos. Differences in financial budgets, timelines and priorities between the two sectors create misalignment in goals and strategies for advancing quantum technologies. Without addressing these gaps and fostering collaboration, both sectors risk further fragmenting efforts and missing collaborative opportunities for advancements across the quantum ecosystem.

Incentives and Market Forces

A key challenge in adopting PQC is motivating organizations to transition. Survey data from stakeholders across government, industry and academia confirm this challenge: 80 percent of respondents in the Vision for the Future of Quantum Technologies survey conducted by CIGI called for accelerating the transition to PQC standards, identifying it as a top priority for long-term cryptographic resilience (Forrest and Murphy 2025).

While organizations often delay migration in the absence of immediate mandates or regulations, selling to governments can act as a strong incentive for companies to transition, as compliance with cryptographic standards can be required for securing procurement contracts. Market forces also create pressure to expand PQC adoption globally, ensuring interoperability with existing services and products. In many cases, market norms establish informal industry expectations, further encouraging companies to align with evolving standards.

Despite these incentives, technology-switching costs remain a significant disincentive. Setting regulations for PQC adoption, as seen in the United States, could address this hesitation. Given the close economic and technological ties between Canada and the United States, American regulations are likely to positively influence Canada's transition to PQC, fostering alignment and interoperability across the two nations.

Market-Driven Standards Development

Efforts such as those by NIST to create standards have mainly been driven by commercial interests. Corporations repeatedly urged NIST to develop standards for PQC as a cost-saving mechanism. With NIST leading the effort to set standards, companies saved time and money they would have otherwise spent on standardization, especially since they may lack the necessary cryptographic resources and expertise.

Despite these efforts, companies are reluctant to invest in stronger security measures unless mandated by regulatory bodies. PR3, who oversaw security for a major airline, explained that while the quantum threat could impact operations control, it is not an immediate priority, as its effects are expected to be years away. PU1, specializing in standardization governance and quantum technology policy, emphasized that companies often adopt a "wait until necessary" approach in the absence of regulations mandating a transition, since security is not typically a feature that businesses can directly sell to their customers.

The "wait until necessary" mindset is also evident in the regulatory and legal aspects of PQC. A1 shared that in a discussion about the legal and regulatory implications of PQC among an assembly of cryptographers and business executives, the cryptographers argued that current laws must change, as they are inadequate for addressing the risks of PQC. By contrast, corporate executives shared that when data is compromised and leads to a lawsuit, they would prefer a reactive approach led by their legal team, rather than a proactive approach to address risks such as SNDL that protects consumer data in advance.

Leveraging Market Forces

Since implementing PQC offers no immediate financial gain and involves significant costs, many organizations are hesitant to transition. PU1 compared this reluctance with the US government's approach, which is more proactive: The government mandates the transition to PQC for federal agencies and partner organizations. This model of enforced compliance sets clear expectations for businesses, reducing uncertainty and motivating action.

The requirement to adopt PQC for securing federal contracts can help motivate organizations. PU2, a subject matter expert on cryptography and cybersecurity regulations in Canada, emphasized that the prospect of selling to the government is a significant driver. This demand-driven approach illustrates how market forces push companies to meet standards — such as certified cyber software — to stay competitive. By positioning governments as major customers, regulatory bodies can indirectly encourage businesses to comply with cryptographic requirements, including transitioning to PQC, without imposing direct regulations. PU2 also pointed out that industries such as banking, motivated by profit, prioritize strong cybersecurity to maintain customer trust and profitability.

Market pressures may also influence the global scope of PQC adoption to allow for interoperability with existing services. PU2 stated that to successfully operate in global markets such as Canada, Europe, India, Japan and the United States, it is essential for businesses to ensure their systems and technologies are compatible and work seamlessly across different regions. This interoperability allows products and services to meet international standards and cater to markets globally. The need for seamless integration across international markets puts additional pressure on

corporations and governments to define and align their strategy for the transition to PQC. This creates a positive feedback loop, where market-driven global collaboration becomes essential for effective implementation.

Informal Deterrents and Herd Behaviour

Norms and market forces may also serve as informal modes of regulation. A3 raised concerns about fairness and accessibility in tiered services, questioning whether organizations might charge more for PQC, thereby prompting considerations of equity and accessibility. In a tiered-service model, companies offer different levels or packages at varying price points. If PQC is only included in the higher-priced tiers, individuals or organizations with limited resources may be left with weaker security options, raising concerns about unequal access to essential cybersecurity measures.

At the same time, they note that market norms can create industry expectations and informal market standards that are not formal regulations. A3 used the example of the health-care sector, where if four out of five hospitals were using PQC, it would raise questions as to why one hospital is not. This creates a dynamic where adopting PQC becomes both a technical necessity and a competitive advantage while also fostering trust among users and customers.

PR4, an expert in global standards for wireless and emerging technologies, provided the example of organizations switching to a new system to reduce operating costs, which may seem beneficial until the cost of the transition is considered. They stated the biggest challenge for the private sector in implementing PQC is that they will not do anything until they need to. Providing organizations with clear incentives is thus essential for alleviating concerns about cost, resources and skill investments.

The severity of resource constraints varies by sector. Organizations in data-intensive sectors such as health care may have systems that are vulnerable to current cybersecurity concerns as they are not adequately protected against modern cyberattacks. Transitioning to PQC could require these organizations to rearchitect their infrastructure, which would be costly.

Regulation and Global Markets

Governments can accelerate the adoption of PQC by establishing clear regulatory frameworks. In the United States, federal legislation, specifically the Federal Information Security Modernization Act, originally enacted in 2002 and amended in 2014, requires government agencies to adhere to information security standards developed by NIST.[4] PU3 explained that Canada should adopt a similar approach to ensure data security, particularly for sensitive information such as financial and health-care data. Regulation in this area is critical, as breaches could have severe implications for national security.

The White House issued a National Security Memorandum (NSM-10) requiring organizations to adopt PQC to remain on the approved vendor list (The White House 2022a, 2022b). A1 explained that the White House directive on PQC galvanized vendors, creating a sense of urgency to demonstrate their readiness. By contrast, A1 observed, Canada's response appears quieter. When A1 asked senior Canadian officials why there was no counterpart to US President Joe Biden's executive order,

4 See https://csrc.nist.gov/Projects/risk-management/fisma-background.

they replied that — although their efforts are less public — the sense of urgency is comparable and substantial work is under way behind the scenes.

Historically, Canada has benefited from emulating or shadowing US policy: When American vendors upgrade their cryptographic offerings, Canadian firms that are integrated into the same supply chains can adopt those solutions quickly and at lower cost. Yet recent political and economic volatility in the United States, coupled with periodic threats to Canadian sovereignty, makes overreliance on US leadership increasingly risky.

The European Union, meanwhile, has set out a clear migration timeline. A road map released in June 2025 directs member states to start their transition to PQC by the end of 2026. It also requires PQC to be implemented for high-risk sectors, such as critical infrastructure, by 2030, and aims to complete the transition of most remaining systems by 2035 wherever feasible (NIS Cooperation Group 2025).

The recent announcement of the new EU-Canada strategic partnership highlights plans to pursue collaboration on tech-policy issues. It also focuses on emerging technologies such as quantum and calls for the alignment of regulatory frameworks and standards. The new EU-Canada Security and Defence Partnership broadens cooperation on cyberthreats and other security matters, creating an umbrella under which future joint work on cryptographic resilience may fit (Prime Minister of Canada 2025).

Given the geopolitical and commercial complexities of emerging quantum technologies, the CIGI survey underscores the need for multilateral engagement. Survey respondents called for greater use of international fora to promote secure and equitable quantum development, including through shared market access, interoperable standards and coordinated regulation (Forrest and Murphy 2025).

Federal Canadian agencies may therefore consider complementing their ties to US agencies by deepening engagement with the European Union and other multilateral standardization and certification bodies (see Table 2). Aligning with EU initiatives not only diversifies Canada's regulatory reference points but also positions Canadian firms to meet the stringent requirements of the General Data Protection Regulation (GDPR) and other emerging EU cyber-resilience legislation — standards that are likely to shape global markets.

Canada's current "adequacy" designation under the European Union's GDPR — built on the Personal Information Protection and Electronic Documents Act (PIPEDA) — already allows Canadian products and services to circulate freely in Europe without additional certification. Strengthening regulatory convergence with the European Union would preserve this advantage, future-proof Canadian exports and mitigate the geopolitical risks that come from depending too heavily on a single partner. Appendix 4 provides further details on PIPEDA and Canada's adequacy status.

Table 2: Overview of Regulation, Standardization and Certification in PQC Adoption

Aspect	Regulation	Standardization	Certification
Definition	Legally enforceable rules set by the government to ensure compliance with PQC requirements.	Development of universally accepted technical specifications.	Verification process ensuring cryptographic modules and IT security products meet established standards.
Primary goal	Enforce PQC adoption to ensure national security and cybersecurity resilience.	Create a common framework for secure and interoperable PQC implementation.	Provide assurance that cryptographic products meet security and compliance requirements.
Key actors	• Governments and regulatory bodies (for example, US Congress, European Commission, Canadian government). • Cybersecurity agencies (for example, CISA, National Security Agency [NSA], Communications Security Establishment [CSE]). • Sector-specific regulators (for example, Office of the Superintendent of Financial Institutions [OSFI] for banking in Canada).	• Standards organizations (for example, NIST, International Organization for Standardization [ISO], ETSI).	• NIST and Canadian Centre for Cyber Security (the Cyber Centre) Cryptographic Module Validation Program (CMVP): certify cryptographic modules under the Federal Information Processing Standard (FIPS) 140-3 based on test results from accredited labs. • National Voluntary Laboratory Accreditation Program (NVLAP): accredits independent labs for cryptographic testing. • NVLAP-accredited cryptographic testing labs: conduct FIPS 140-3.[5]
Challenges	Slow legislative process; potential issues surrounding interoperability between national and international regulations.	Difficulty achieving global consensus; evolving PQC landscape requiring ongoing updates.	Costly and time-consuming for vendors; potential bottleneck in certification processes.
Examples	• NSM-10: sets PQC migration guidelines for federal agencies. • Quantum Computing Cybersecurity Preparedness Act: mandates federal agencies to inventory quantum-vulnerable systems.	• NIST PQC Standards (FIPS 203, FIPS 204, FIPS 205): define new cryptographic algorithms (NIST 2024).	• FIPS 140-3 certification: mandatory for cryptographic modules used in US federal agencies to ensure they meet FIPS certification requirements (NIST 2019). • Common Criteria certification: used internationally and recognized by member countries of the Common Criteria Recognition Arrangement, allowing certified IT security products to be accepted across participating nations.[6]
Impact on adoption	Drives compliance but may lack agility for innovation.	Ensures interoperability and guides industry best practices.	Builds trust in PQC solutions for secure applications.
Recommended timeline (as per US NSA)[7]	**2024–2035**: Phased PQC adoption in federal agencies per NSM-10, with full compliance required by 2035.	**2024–2031:** Standardization of PQC algorithms, industry adoption and deprecation of legacy cryptography.	**2024–2035:** Gradual certification of PQC implementations under FIPS 140-3, with full compliance required for cryptographic modules by 2035.

Source: Authors.

5 See https://csrc.nist.gov/projects/cryptographic-module-validation-program.

6 See www.cyber.gc.ca/en/tools-services/common-criteria.

7 See NSA (2022).

Standards, Certification and Regulation

This section details the regulatory processes for PQC adoption. The authors begin by outlining how PQC is standardized, including the certification process for PQC algorithms and its associated challenges. Next, they discuss the accessibility of PQC standardization, including patents and licensing agreements for implementation. The authors then address the challenges of establishing regulations and the role of standardization in PQC adoption. Finally, they evaluate current regulatory approaches taken by various jurisdictions and the challenges they present in assessing their effectiveness as potential regulatory models.

Cryptography standardization is a multi-step process designed to ensure the development, evaluation and implementation of secure and reliable cryptographic systems. Standardized certification is important to ensure security and build trust in new technologies. A consistent theme emerging from expert interviews was the need for standardization prior to regulation in the early stages of PQC adoption. Experts emphasized that regulations may be premature at this point, given the recent release of the NIST standards, which lay the groundwork for testing and certifying cryptographic schemes. Standardization involves a collaborative process between academic researchers, bodies such as NIST and policy-setting agencies to thoroughly evaluate, certify and deploy cryptographic technologies. While this process provides a foundation for secure adoption, challenges remain, such as navigating adoption timelines and determining the balance between eventual regulation and government mandates.

The Standardization Process

PU2 and A4 outlined the logistical process and the stakeholders involved in transitioning to PQC. The process starts by identifying a long-term threat, which requires building new cryptographic algorithms. The first step is developing candidate mathematical problems on which cryptographic schemes are based. These problems are studied extensively by the academic research community to assess their security and ensure they are difficult to break. Once promising candidates are identified, cryptographic primitives[8] such as public-key encryption and digital signatures are built on these foundations.

These designs are then subjected to public scrutiny through peer review and formal standardization processes, such as the NIST initiative. In the NIST PQC standardization process, many algorithms were submitted and evaluated over multiple rounds of public review, ultimately narrowing the candidates to a small set of algorithms that withstood scrutiny. These selected algorithms are then standardized by various regulatory bodies. Following this, the attention shifts to integrating standardized algorithms into applications and systems, such as network protocols (for example, Transport Layer Security [TLS] or PKI for managing public keys).

Next, algorithmic implementations are developed, such as updates to web browsers,

8 Cryptographic primitives are simple cryptographic algorithms that serve as a foundation for more advanced cryptographic algorithms. See https://csrc.nist.gov/glossary/term/cryptographic_primitive.

web servers and software development kits, which are then evaluated and deployed to users. Alongside these technical steps, policy and regulatory efforts play a role in identifying the need to transition and driving organizations to adopt these technologies, despite associated costs.

In Canada, the government plays two roles in PQC adoption: It acts as a policy-setting body and a consumer of technology. Agencies such as the Cyber Centre, CSE and the Treasury Board Secretariat (TBS) set cryptographic policy for the Canadian government. These agencies determine which security requirements systems must meet. As noted by A4, Canada often chooses to adopt NIST standards. However, as NIST is an American non-regulatory standardization body, Canada can make its own choices.

The Role of Canadian Regulatory Bodies

The Cyber Centre oversees communications equipment for sensitive and classified information on behalf of the Canadian government. The agency collaborates with departments such as the TBS and Shared Services Canada to develop and implement cybersecurity guidance. For instance, the TBS oversees policies for the Government of Canada's security framework and is responsible for the enterprise cybersecurity strategy, which is available publicly. While the Cyber Centre offers recommendations to the TBS, such as suggested cryptographic key lengths or adherence to NIST or ETSI standards, the TBS has the authority to mandate specific requirements for federal departments.

The Cyber Centre also conducts applied research in cryptography and publishes guidance documents available to all Canadian organizations. While these recommendations were initially tailored for government use, they have expanded to include general guidance for any organization in Canada. For example, the Cyber Centre released publicly available documents on quantum technologies and PQC, ensuring that organizations outside the government can benefit from best practices.

PU2 explained that the guidance can and should be used by any Canadian organization. In addition to guidance, the Cyber Centre also contributes to certification. The Cyber Centre and NIST jointly manage a program in which they certify test labs. Much of the program runs under the FIPS 140, which ensures the quality and security of cryptographic products. FIPS 140 is a US government standard that outlines baseline security requirements for cryptographic modules in IT products, with modules validated under this standard by NIST and the Cyber Centre.[9] Through this program, companies that have cryptography products can take their products to private test labs to be certified. These test labs evaluate the cryptographic products of companies to ensure proper implementation and adherence to standards. A more detailed explanation of the certification process can be found in Appendix 2.

Certification and Standardization Challenges

PQC implementation relies on effective standards, certifications and regulations. A3 highlighted challenges in standardization, noting the lack of a clear adoption road map across industries. This uncertainty hinders organizations, especially critical infrastructure providers, from adopting necessary standards to address quantum threats. PU2 emphasized the role of certification as a vital, non-regulatory approach

9 See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/use-of-fips-140-2-logo-and-phrases.

to ensuring cryptographic reliability. While not enforceable, certification encourages standardized cryptographic solutions. Recommending certified cryptographic products helps push the market toward best practices, setting the groundwork for secure and reliable implementations. The creation of standards sets the groundwork for testing and certification, making sure organizations can implement reliable and secure cryptographic solutions.

However, certification processes come with their own set of challenges, given the diverse range of programming languages, libraries and implementations that must be evaluated. PR8 explained that while these processes are resource-intensive and time-consuming, they are essential for ensuring the reliability of cryptographic solutions. Governments and high-security environments rely on these certifications to classify systems as secure, emphasizing the need for rigorous evaluations.

Balancing Standards, Patents and Accessibility in PQC Adoption

Standards are essential for widespread adoption, providing a foundation accessible to all, including companies not involved in their creation. However, PU1 highlighted complexities in commercializing standards due to intellectual property rights (IPR). Contributions to standards may be protected by patents, and companies implementing these standards must obtain licences from patent holders.

This system allows contributors to recoup their investments over time. While standards are freely available for reference, commercial use requires licensing. PU1 noted licences can be obtained through patent pools, where patent holders collectively offer a single access point for implementers (World Intellectual Property Organization 2014). This process simplifies acquiring rights and avoids negotiating individual agreements. Without a patent pool, companies must identify patent holders and secure separate licences, complicating commercialization. Despite its complexity, this system ensures IPR compliance and supports the commercialization of standardized technologies.

The Cryptographic Suite for Algebraic Lattices–Kyber algorithm, chosen by NIST for its PQC standards, demonstrates how licensing can simplify the use of patented technologies in commercial applications. To encourage adoption, NIST collaborated with US and French patent holders to allow free use of the algorithm, as long as organizations follow the specified terms. This approach removes intellectual property barriers, fosters global collaboration and supports the development of secure cryptographic solutions for a post-quantum future (NIST 2022).

Regulatory and Policy Dynamics

Many experts believe that while regulations are necessary, it may be too early to implement them. The recent Group of Seven (G7) Kananaskis declaration on quantum technologies reinforces this view, noting that we are still in the early stages of innovation, which makes global regulatory frameworks premature. However, the shared vision calls for a timely transition to QSC to secure existing communication networks (G7 Leaders 2025).

A1 argued that the focus should not yet be on regulation, as quantum-resistant PKC algorithms are still undergoing standardization, and there are still vulnerabilities being discovered in PQC.

While discussing PQC implementation challenges noted in the literature, PR4 emphasized that regulations alone will not address key issues such as the need for increased processing power, high latency, incompatibility with existing systems and the lack of conclusive testing. However, they view certification as a valuable tool, as it avoids the implication that one institution's security systems are inherently better than another institution's. They also highlighted the work of NIST and ETSI in proving the security of algorithms through rigorous evaluation processes that include simulations, computational cycle measurements, and tests of hardness and breakability. Adjustments to parameter sets, such as reducing key sizes, often reveal vulnerabilities, demonstrating the importance of certification in ensuring security across various implementations. PR4 stressed that when the time comes for regulation, there must be flexibility, as every organization, company and government has different needs and circumstances.

Standardization is likewise identified as a critical step before organizations can begin implementing tailored PQC solutions. PR1 emphasized that effective regulation involves first standardizing alternatives for cryptography at the core of IT security, which includes signature schemes and key encapsulation or key exchange mechanisms. Beyond these primitives, additional cryptographic building blocks will also need to be developed and standardized.

Outcome-Focused Cryptography Regulation

While experts had differing views on how to manage and regulate cryptography, one common thread was the need for a flexible, results-driven approach to security rather than enforcing rigid mandates. This is due to the varied contexts in which cryptography is implemented. PR5 and PU5 emphasized the limitations of traditional regulation while expressing the benefits of having an incentive-driven approach that aligns regulatory requirements with business needs.

Flexible Approaches to Cryptography Regulation

PU5 reflected on past attempts to regulate cryptography, observing that such efforts often fail and tend to worsen rather than improve security and privacy; for example, regulations targeting specific aspects — such as key escrow[10] or encryption strength — have historically been ineffective. Instead, they advocate for an outcome-based approach where organizations are evaluated on their ability to achieve and maintain security, rather than adhering to rigid rules. In the United States, agencies

10 See https://csrc.nist.gov/glossary/term/key_escrow_system.

such as the Department of Health and Human Services can penalize health-care providers for breaches caused by negligence in protecting data. However, providers can avoid penalties by demonstrating the use of secure encryption methods, such as NIST-approved standards, which showcase responsible and proactive data protection. This approach encourages organizations to adopt effective practices while allowing flexibility and avoiding the drawbacks of overly rigid regulation.

PU5 also highlighted the risks of universally mandating encryption, pointing out that in certain situations, encryption may not be the optimal solution. They cited examples of resource-constrained environments, such as real-time systems in factories or plants, where strict encryption requirements could lead to operational issues such as latency. PU5 proposed the idea of compensating controls, which provide organizations with alternative ways to meet security goals when encryption is not a suitable option. These controls allow organizations to implement cost-effective solutions tailored to their needs, avoiding the challenges of outdated or rigid regulatory requirements. By offering more options to achieve the same security outcomes, compensating controls enable organizations to maintain security without compromising efficiency.

Comparing Proactive and Reactive Regulatory Approaches

Outcome-focused regulation stands in contrast to the reactive regulatory approach often seen in the United States, where technology adoption is mostly shaped by market demands. PU5 noted that in the United States, regulation typically only occurs in response to demonstrated market failures. In contrast, the European Union proactively regulates new technologies, leaving it to the market to adapt within the established framework. In the United States, reliance on market forces can delay essential regulatory changes, and when market failures happen, the reactive approach often fails to address the gap effectively.

Echoing the European Union's proactive stance, the recently released PQC migration road map sets deadlines for high-security sectors such as critical infrastructure, creating a strong external driver for wider adoption. In line with the European Union's approach, A4 highlighted the critical role that regulations will play in standardizing the transition to PQC. For larger, well-prepared organizations, such regulations will enforce specific timelines and ensure compliance with established standards. At the same time, these regulations are essential for smaller, less-prepared organizations in the private sector, such as credit unions, which may not yet be aware of or ready for the necessary changes. While Canada's major banks are likely already on track with PQC adoption, smaller institutions may need regulatory pressure to align with the broader transition to QSC.

However, some experts view regulatory "forcing power" as a critical aspect of effective cryptography regulation. The lack of strong enforcement mechanisms in the United States complicates this effort. PR5 explained that while initiatives such as NSM-10 and an executive order mandate migration to PQC, they lack penalties or incentives to drive compliance. They use the Payment Card Industry Data Security Standard as an example of effective enforcement, where non-compliance results in losing access to essential services such as credit card processing. Without similar enforcement mechanisms for PQC, progress remains slow.

Challenges in US PQC Regulation and Implementation

Regarding the US government's approach to regulating PQC, PU2 commented on the mandate for federal departments and partner organizations to transition to PQC by 2035. They noted that meeting this timeline will be challenging, as PQC algorithms are only recently standardized and certified products are not yet available. However, they also pointed out that the government has faced similar challenges before, such as when cryptographic algorithms were deprecated faster than expected.

Comments made by PU2 and PR5 are supported by a recent report from the Government Accountability Office (GAO), which highlights the difficulty of transitioning to PQC in the United States. The report highlights challenges due to the lack of a centralized entity overseeing PQC migration, warning that the federal government's shift to PQC may fail without a single authority coordinating a national strategy to address the quantum threat. It recommends that the Office of the National Cyber Director lead federal agencies through the PQC migration process and beyond. While the government has spent the past eight years issuing guidance documents from multiple agencies, the GAO points out that the lack of centralized leadership hinders progress.

The GAO identifies three primary goals for this strategy, which has yet to be fully addressed due to the absence of a single federal organization responsible for coordinating the effort (GAO 2024):

- standardizing PQC;
- migrating federal systems to PQC; and
- encouraging the broader economy to prepare for quantum threats.

To achieve these goals, the strategy must define the problem, assess risks, outline clear objectives and activities, and establish milestones and performance measures.

Varying Regulatory Frameworks

This section examines different regulatory approaches across jurisdictions, focusing on cryptography regulation in Canada and the roles of governing bodies. It compares Canada's regulatory framework with those of the United States and the European Union, highlighting key factors such as sovereignty concerns and global system interoperability. The section concludes with Canada's potential role in the global transition to PQC.

Regulatory approaches to PQC vary across regions due to differences in governance structures, economic priorities and geopolitical factors. In Canada, cryptography regulation is divided by sector and jurisdiction, presenting both challenges and opportunities. Comparisons with the United States and the European Union reveal significant differences in their approaches. Sovereignty considerations influence standards adoption, shaping each nation's regulatory priorities.

These diverse approaches complicate efforts to ensure interoperability and foster international collaboration. As quantum technology advances, addressing these

differences will be crucial for global security. Canada has an opportunity to play a leading role in PQC adoption by driving migration efforts and promoting alignment with international standards.

How Is Cryptography Currently Regulated in Canada?

In Canada, the TBS is responsible for shaping and implementing cybersecurity strategies for government. PU2 explained that TBS, working closely with the CSE, develops policies that serve as both guidance and a framework for government operations. Like NIST in the United States, the types of guidance offered by TBS and CSE, while influential, are recommendations and are not enforceable mandates.

These guidelines are publicly accessible and provide information for organizations regarding PQC and preparing for the quantum threat. Additional details regarding these documents and their associated standards can be found in Appendix 3.

The use and regulation of cryptography is sector dependent. For federally regulated financial institutions (FRFIs) — such as banks, loan providers and life insurance companies — the OSFI provides guidance on the use of secure cryptographic technologies to protect their systems. OSFI advises FRFIs to protect encryption keys throughout their key management life cycle as well as regularly reviewing and updating their cryptographic standards and technologies to ensure they are effective in addressing current and security threats (OSFI 2022; Government of Ontario 2025). While these guidelines do not apply to private businesses, they do apply to vendors and third parties under contract with the Ontario government.

Fragmented Governance and the Challenge of Coordinating PQC in Canada

While the United States has NSM-10, which outlines a national strategy for advancing quantum computing leadership and managing risks to cryptographic systems, Canada operates under a more fragmented regulatory framework involving multiple bodies overseeing various sectors. In Canada, the responsibilities are divided between federal and provincial governments, with federal jurisdiction covering telecommunications, transportation and financial institutions, among others, and health and education falling under provincial authority.

Federalism poses challenges for establishing unified timelines and strategies for adopting PQC across the country. For example, telecommunications are regulated by ISED, and the OSFI guides system protection for financial institutions. These sectors, though not without complexity, benefit from relatively clear federal jurisdiction and national oversight, making them more straightforward for a federally led transition. By contrast, sectors of provincial jurisdiction, such as health care, public education and municipal services, are more difficult to coordinate. Especially in larger provinces, there is a wide variety of local and special-purpose governing bodies (for example, municipalities, school and hospital boards, regional health governments, public health units) that operate with varying degrees of financial flexibility and human capacity to implement major system changes. These sectors also involve vast volumes of sensitive data with long shelf lives, adding further complexity to any system-wide cryptographic upgrade.

Segmented regulatory oversight also poses challenges for enacting privacy laws, as it raises questions about who has the power to mandate the PQC transition. The development of clear legal frameworks tailored to address quantum-specific challenges is crucial, but it remains an ongoing process. In practice, federal guidance may be limited in its ability to compel adoption in sectors that are governed primarily at the provincial or municipal levels. This highlights the importance of sustained intergovernmental cooperation, particularly in areas where national coordination is essential to securing distributed systems.

Various departments of the Canadian government have issued strategy documents or road maps that focus on, or at least mention, the adoption of PQC. While Canada's NQS notes the transition to PQC, the Cyber Centre has released an updated road map to guide the Government of Canada's migration. These documents set timelines for developing a department-wide migration plan by April 2026, fully migrating high-priority systems by the end of 2031 and completing the migration of remaining systems by the end of 2035 (ISED 2025; the Cyber Centre 2025a).

The Department of National Defence and Canadian Armed Forces (DND/CAF) have released a Quantum S&T Strategy implementation plan, known as Quantum 2030. Following the release of the NIST standards, DND/CAF and the CSE are coordinating with allies to deploy PQC. This coordinated effort will enable interoperability with allied systems (DND/CAF 2023).

When discussing how Canadian government departments coordinate PQC implementation, PU2 described a well-established process for sharing advice and guidance. CSE publishes recommendations for government departments and shares them with critical infrastructure and industry partners. Extensive outreach within the cybersecurity community focuses on encouraging the adoption of certified cryptographic standards and mitigating risks such as SNDL attacks, even while using traditional PKC.

This outreach includes strategies to address current threats and practical advice for transitioning to PQC. CSE can continue to provide updated resources and guidance to support organizations throughout the PQC migration process. Organizations are encouraged to work with service providers to incorporate PQC-compliant cryptography into future contracts and systems once standardized products become available. However, the ability to act on such guidance will vary significantly across sectors and jurisdictions, particularly in those where institutional fragmentation and limited capacity create barriers to implementation.

Global and Sovereignty Considerations

Regarding global adoption, PU1 suggested that NIST standards are likely to become widely accepted across Western countries and beyond, with nations such as India and Japan also expected to adopt them. However, they point out that regional differences may persist, particularly with countries such as China pursuing alternative standards. This divergence raises concerns about global interoperability, emphasizing the need for collaboration during the standardization process to avoid fragmentation. Different PQC standards across countries can hinder global interoperability by creating incompatibility between systems, increasing costs for organizations managing multiple standards and weakening international security coordination. However, varying cryptographic standards are often necessary, as different commercial and government markets have distinct security, regulatory and operational requirements that shape their choice of cryptographic solutions (Leech and Chinworth 2001).

Through the Kananaskis Common Vision statement and the G7 Finance Ministers and Central Bank Governors' Communiqué, nations have signalled joint efforts to explore the policy implications of quantum technologies. The G7 Joint Working Group on Quantum Technologies will advance policy discussions on innovation and adoption strategies, encouraging wider cooperation and engagement. Meanwhile, the G7 Finance Ministers and Central Bank Governors' Communiqué examines how quantum technologies could reshape global finance and calls for the evaluation and reduction of information security risks (G7 Leaders 2025; G7 Finance Ministers and Central Bank Governors 2025).

Geopolitical considerations play a significant role in shaping PQC adoption, with concerns about sovereignty influencing regulatory decisions. PR8 highlighted Europe's efforts to reduce reliance on US vendors through sovereignty initiatives that keep processes and resources within the region. They noted that protectionism and geopolitical tensions complicate international collaboration, particularly in accessing global talent to support migration.

Given people's limited expertise in PQC, PR8 explained that while talent can be outsourced across European nations, it cannot extend beyond European borders. These tensions, driven by global conflicts, are fuelling polarization and protectionism, which may hinder long-term progress in technological innovation.

Interoperability and International Collaboration

Different regulatory frameworks across jurisdictions can affect standard compatibility, making interoperability and international collaboration essential for seamless communication and security. Global alignment of standards is critical to ensure interoperability with current and emerging technologies. A2 highlighted the advantages for companies such as Amazon in adopting global standards, emphasizing that a unified framework benefits everyone. Similarly, A3 underscored the need for compatibility across national standards, warning that diverging standards could create significant interoperability challenges.

In the defence sector, these challenges are even more pronounced, adding to existing barriers to interoperability such as strict security controls, complex regulations and limited vendor ecosystems that already make military networks difficult to link. This becomes exponentially harder when allied nations operate on incompatible communication standards (Parker 2025). To preserve reliable information exchange as they shift to PQC, allies must coordinate on shared standards, preventing the fragmentation that could otherwise undermine military communications. The transition to PQC will require extensive collaboration among nations and between the public and private sectors (see Table 3). PR4 stressed the importance of international cooperation, likening it to the past standardization of IT systems, which enabled smooth global integration. They argued that national standards are largely irrelevant, except in specific local sectors such as health care. Using the example of the Robertson screwdriver — unique to Canada — PR4 illustrated the inefficiency of isolated national standards in a globalized world.

Table 3: Comparative Analysis of National Approaches to PQC Migration Preparedness

Dimension	Canada	United States	United Kingdom	European Union
Regulatory framework	No centralized PQC mandate. TBS and CSE oversee government migration and provide guidance while sector-specific regulators manage industry-specific policies.	NSM-10 mandates phased PQC adoption in federal agencies.	The National Cyber Security Centre (2024) provides guidance and recommendations on the migration.	The European Commission recommends member states develop a strategy. Each member state is responsible for national implementation (European Commission 2024).
Standardization efforts	The Cyber Centre is collaborating with NIST but does not have an independent national PQC standardization program.	NIST leads PQC standardization and FIPS certification efforts.	.The United Kingdom aligns with NIST standards.	ETSI, ISO and national standardization bodies such as BSI in Germany.
Implementation timeline	Timelines set within the Government of Canada to determine department migration plans by April 2026, migrate high-security sectors by the end of 2031 and migrate remaining systems by 2035 (The Cyber Centre 2025a).	2024–2035 for phased federal PQC adoption per NSM-10, with full compliance required by 2035.	Organizations in industry, government and critical national infrastructure should have a migration plan by 2028, with the highest-priority systems migrated by 2031 and all systems migrated by 2035 (National Cyber Security Centre 2025).	Member states should have a national PQC transition strategy by the end of 2026, ensure that high-risk use cases migrate by the end of 2030 and transition as many systems as feasible by 2035 (NIS Cooperation Group 2025).
Challenges and barriers	Tight migration timelines with a large-scale migration focused primarily on the government.	Tight migration timelines with a large-scale migration.	Tight migration timelines require defining migration strategies by 2028 for organizations with large-scale migrations.	Tight migration timelines while also coordinating the approach by each member state with limitations in finances and expertise (De Luca 2024).

Source: Authors.

Canada's Role in the Global Context

Canada's role in the global quantum ecosystem highlights its potential to influence international standards. Canada can help lead the transition to PQC by initiating and fostering global discussions on PQC adoption, ensuring a collaborative approach to implementation.

This leadership is reflected in several recent policy initiatives. Canada's NQS, released in 2022, identifies "quantum communication and post-quantum cryptography" as one of three core missions. The strategy emphasizes international partnerships, coordination between public and private sectors, and support for foundational research and talent development.[11]

The Government of Canada has since released a quantum communication and PQC road map (ISED 2025), which outlines concrete activities such as piloting quantum-safe solutions, promoting interoperability and raising awareness among system owners (ibid.). These initiatives are further supported by a federal PQC migration road map (ITSM.40.001), which outlines the following clear milestones (The Cyber Centre 2025a):

- April 2026 — departmental migration plans due;
- 2031 — migration of high-priority systems; and
- 2035 — full migration of non-classified federal IT systems.

These strategic documents provide a basis for Canada to engage internationally by hosting meetings with policy makers, facilitating informal consultations with international representatives and contributing to a global quantum-safe forum. A3 suggested that Canada can also lead by leveraging its strong research community to advocate for higher security standards, aligning with existing norms or contributing to new ones. Achieving this requires continued collaboration among industry stakeholders, universities and policy makers to establish a coordinated national stance and play a meaningful international role.

Recent academic analysis highlights a shift in Canada's quantum posture from a balanced view of opportunity and threat to a more securitized narrative, particularly in the transition from earlier strategies to the DND/CAF Quantum 2030 implementation plan (Murphy and Parsons 2024). This trend may constrain democratic oversight by framing quantum policy as the exclusive domain of technical experts (Murphy and Parsons 2025). While acknowledging legitimate security concerns, the authors advocate for desecuritization to ensure that public debate informs investment decisions, oversight mechanisms and the ethical governance of dual-use technologies.

This is especially relevant in light of Prime Minister Mark Carney's June 2025 announcement to raise defence spending to two percent of GDP, which is expected to include major investments in secure digital and quantum infrastructure (DND 2025). As quantum capabilities become increasingly embedded in national security planning, it will be important to ensure that democratic accountability remains a central principle in shaping Canada's quantum future.

11 See https://ised-isde.canada.ca/site/national-quantum-strategy/en.

Evaluation of Public-Private Sector Roles in Canada

The public and private sectors have distinct yet complementary roles in adopting PQC. Governments establish regulatory frameworks, provide guidance and ensure critical infrastructure prioritizes security, while the private sector drives innovation, develops solutions and implements these technologies. However, inconsistent awareness within governments and differing priorities between sectors pose challenges.

A lack of centralized resources for industry leaders to address emerging threats, alongside competing priorities, further complicates the process. The public sector must take the lead in guiding a unified approach, while joint initiatives can align priorities and readiness levels to ensure a seamless transition to PQC. Informal information-sharing and collaboration through structured gatherings can help bridge these gaps.

Issues Regarding Public-Private Sector Alignment

Addressing complex, long-term technological challenges such as quantum computing will require effective alignment between the public and private sectors to allow the sharing of knowledge, best practices and learned lessons. However, the challenge remains in achieving this alignment to foster collaboration due to varying priorities and limited resources. A1 noted that public sector organizations cannot be grouped into a single category due to inconsistencies in their expertise, readiness and awareness regarding quantum technologies. PU6 supported these claims by suggesting that the transition to PQC is not necessarily a topic the entire Government of Canada needs to investigate. Instead, it is the responsibility of specific organizations or sectors within the government.

Highlighting the role of joint public-private sector initiatives, PR6 pointed to the Creative Destruction Lab (CDL) as an example of programs that support the growth of quantum technology start-ups, including those focused on PQC. They explained that CDL nurtures viable businesses by providing resources and support tailored to quantum computing and PQC companies. Alongside these existing support services and its mentorship of quantum technology start-ups, CDL and similar organizations can contribute to the PQC migration by helping data-centric start-ups understand the quantum threat and consider adopting PQC.

Additionally, PR6 highlighted the distinct responsibilities of the public and private sectors in supporting this transition. While start-ups focus on developing quantum technologies, governments must establish policies to address the associated security threats. They emphasize that corporations should adopt PQC as early as possible while governments take charge of creating regulatory frameworks. This division of roles highlights the need for coordination, where private companies depend on public sector policies to guide innovation responsibly.

One organization already facilitating connections in the Canadian quantum ecosystem is Quantum Industry Canada (QIC),[12] a business-led consortium founded in 2019 that unites start-ups and established firms to turn the country's quantum expertise into commercial advantage. This broad industry mandate positions QIC to serve as a potential bridge between government and the private sector as Canada's quantum ecosystem matures.

To further promote collaboration, PU5 described the importance of regular, structured gatherings between public and private stakeholders. They described the current approach of hosting multi-day conferences and workshops, focusing on sharing ideas, exchanging lessons learned and building professional networks without necessarily aiming to produce immediate deliverables. By fostering informal information sharing and interpersonal connections, these events strengthen cooperation and address shared challenges across sectors.

In contrast, PR3 addressed a key barrier to alignment: the lack of consolidated resources for CIOs to stay informed on emerging technologies. PR3 suggested that a crucial gap in aligning the two sectors is the absence of dedicated resources or centralized knowledge hubs for technology leaders to stay updated. Many CIOs rely on a time-consuming, fragmented approach, taking the initiative to gather their own information from educational sources due to the lack of a structured method for sharing knowledge. This fragmented approach adds to the time pressures CIOs face, forcing them to balance learning about long-term technologies such as quantum computing with their immediate responsibilities.

The absence of such resources limits CIOs' ability to engage deeply with emerging technologies, highlighting the need for better alignment and support mechanisms to integrate long-term technological planning into their roles.

Public-Private Cooperation

Standardization and interoperability require close collaboration between the public and private sectors. While the private sector concentrates on developing and selling products that comply with certification requirements (such as FIPS standards) tailored to specific data rates and security needs, the public sector must prioritize key areas, continuously assess risks and provide guidance for the transition. PU3 emphasized the need for public-private collaboration, highlighting the public sector's role in leading by example.

Organizations such as the Bank of Canada demonstrate this approach by conducting their own PQC readiness exercises, which helps to establish standards, provide oversight and create regulations.

The public sector also plays a critical role in funding and education to support private sector adoption. A3 described the role of government as both educator and enabler, creating opportunities through partnerships with companies and research groups. Such an approach raises awareness and increases access to PQC solutions, particularly for organizations hesitant to invest without clear mandates or timelines.

A2 noted that private companies often view PQC adoption as an avoidable cost unless it aligns with profit goals. In contrast, public sector organizations, such as hospitals, prioritize cybersecurity to protect sensitive data. PR8 agreed, describing private sector hesitation as "laying back and waiting," while the public sector takes a more proactive stance.

12 See www.quantumindustrycanada.ca/about/.

A4 underscored the need for regulations to compel less prepared private sector actors to act. While major banks in Canada are likely ahead in their preparations, smaller institutions, such as credit unions, may lag. Large companies are already anticipating regulations and testing PQC within their infrastructure, but regulatory pressure is vital for ensuring broader adoption among smaller or less advanced organizations.

Conclusion: Policy Recommendations and Next Steps

Given the extensive risks outlined in this special report — including threats to critical infrastructure, financial stability and public safety — federal government leadership in Canada's transition to PQC emerges as both prudent and necessary. The documented vulnerabilities in sectors such as energy, transportation, health care and finance, combined with the considerable time frames required for PQC implementation, underscore the urgency of a coordinated, government-led approach.

Interviews with PQC experts highlighted the inadequacy of voluntary, market-driven initiatives, particularly given private sector hesitations tied to immediate profitability rather than long-term security. Canada's existing cybersecurity institutions — such as the Cyber Centre, CSE and the TBS — already provide robust frameworks for policy formulation, certification and compliance, offering an institutional foundation well suited to manage this complex transition. Moreover, federal leadership is strategically positioned to facilitate alignment with emerging global standards, ensuring interoperability and enhancing international cybersecurity cooperation. These recommendations build on Canada's existing strategic commitments. The NQS and the quantum communication and PQC road map already outline a federal vision for transitioning to quantum-safe systems, including support for standardization, workforce development and global interoperability (ISED 2025; The Cyber Centre 2025a).[13] Therefore, to effectively mitigate quantum threats, the Canadian government must lead regulatory initiatives, establishing clear timelines and requirements to safeguard critical systems and public trust.

In what follows, the authors make recommendations intended for public policy leaders and cybersecurity specialists, presented in a suggested order of implementation, starting with those most urgent for early progress. The authors first highlight the importance of taking early action on PQC, emphasizing the urgency of the migration and developing a plan for its priorities. A second recommendation is to stimulate PQC adoption by training a workforce and providing financial resources. In addition, government procurement can serve as an incentive, while market pressure can encourage global PQC adoption for interoperability with existing services and products. The last section suggests government-led initiatives to guide the migration. To be sure, the necessity for PQC migration is not solely a public-versus-private sector issue but also depends on assessing the hierarchy of risk and data sensitivity, underscoring the importance of collaboration. Ultimately, adoption

13 See https://ised-isde.canada.ca/site/national-quantum-strategy/en.

should be guided by outcome-focused, government-led regulation while strategically leveraging market forces to ensure an effective transition.

A Call for Early Action on PQC Migration

The scale of migrating to PQC necessitates immediate, coordinated action. Based on the outlined risks to critical infrastructure, OT and sensitive civilian data (see the section "Risks of the Quantum Threat"), as well as deployment and regulatory challenges (see the section "Deployment Challenges") — the authors recommend that organizations:

- acknowledge the urgency of PQC migration;
- identify and prioritize sectors requiring transition;
- assess data and security needs; and
- evaluate key factors for PQC algorithm implementation.

Urgency

A major challenge outlined in the sections "Risk Timelines and Technology Life Cycle" and "Urgency and Timelines" is the widespread lack of awareness and underestimation of timelines required for effective PQC adoption. Organizations must recognize that successful PQC migration timelines must factor in the threat of SNDL attacks ("Risks of the Quantum Threat"). Given the unprecedented scale of this cryptographic transition, sectors need to proactively prepare for PQC, accounting for the significant complexity and implementation timelines previously identified. For instance, as explained by Mosca's model, if migration requires five years and data protection is needed for at least five years, quantum-safe solutions must be adopted well before quantum computers become viable — no later than the early 2030s, considering NIST's target of 2035 ("Risk Timelines and Technology Life Cycle").

Organizations should proactively prepare for the adoption of standardized PQC solutions, as detailed in "Risks of the Quantum Threat" and "Deployment Challenges," to ensure a timely and secure transition. Early preparation will help mitigate risks associated with the quantum threat while facilitating the seamless implementation of quantum-safe cryptographic standards. At the international level, in high-security sectors such as finance, the Bank for International Settlements has released a road map outlining a framework to help the financial sector transition to quantum-safe cryptographic systems (Auer et al. 2025). The urgency of PQC migration has also been emphasized in federal guidance documents such as the "Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada," which sets concrete timelines for departments to prepare transition plans and complete system migrations (The Cyber Centre 2025a).

Identifying and Prioritizing Sectors for PQC Migration

As discussed in "Illustrative Quantum Threat Scenarios for Critical Infrastructure and OT," sectors such as government, military, finance, health care, energy and critical infrastructure face significant threats from quantum computing. However, a clear prioritization strategy addressing sector-specific interdependencies has yet to be developed, posing substantial security risks. Given these vulnerabilities,

a consensus must be reached among working bodies on the early adoption of PQC within data-sensitive sectors.

The circulation of data across interconnected organizations ("Illustrative Quantum Threat Scenarios for Critical Infrastructure and OT" and "Public-Private Awareness") must guide prioritization. Organizations do not operate in isolation as many rely on third-party vendors to function securely. For example, if a financial institution is adopting PQC, its payment processors and cloud providers should also transition to avoid vulnerabilities. Since organizations rely on interconnected partners for secure data exchange, prioritizing transitions based on dependencies due to the circulation of data can help mitigate security gaps and establish appropriate migration timelines. This approach facilitates an orderly migration while addressing interdependencies between industries.

Assessing Risks Related to Data and Implementing a Crypto Inventory

Risk-Based Prioritization for Migration

Earlier sections ("Crypto Inventory" and "Crypto Agility and Legacy Systems") identified critical gaps in organizations' understanding of their cryptographic infrastructure, particularly regarding legacy systems and internal vulnerabilities. To address this gap, organizations must perform risk-based prioritization, assessing which data requires immediate quantum-safe security and creating comprehensive crypto inventories. Smaller businesses might not initially prioritize migration, but this determination should emerge clearly from the assessments conducted. The next step is taking an inventory of cryptographic systems, including the types of devices and cryptography in use for each type of data being stored. Creating a cryptographic inventory should be integrated into an organization's broader risk management strategy.

The transition to PQC should be approached as part of a comprehensive risk assessment, which includes evaluating cybersecurity risks, categorizing information assets, and identifying specific security requirements and potential threats. This assessment should also involve determining where data resides and whether it can be sufficiently protected through local storage or secure cloud solutions against quantum-enabled threats.

Legacy systems unable to support new cryptographic standards represent a particular challenge ("Crypto Agility and Legacy Systems") and should therefore receive special attention. While full upgrades may not always be necessary, cryptographic tools can be implemented as an additional security layer to protect communications. Within systems, prioritization is critical, as certain types of data carry higher levels of sensitivity and risk, necessitating earlier migration. For instance, specific sectors within defence departments should be updated before others. This raises the question of whether lessons learned from these prioritized migrations can be effectively communicated and applied to other systems undergoing transition. This urgency of transitioning to PQC also brings into focus whether regulations are needed to facilitate the process. The authors will expand more on whether the migration should be regulated later in this section.

Crypto Agility

Since the standardization of cryptographic algorithms by NIST is relatively recent, there are concerns that some algorithms may be unexpectedly broken in the near future. To mitigate this risk, organizations are encouraged to adopt crypto agility — the ability to switch cryptographic algorithms with relative ease — so that

cryptographic systems can be updated without requiring a complete overhaul. For many organizations, crypto agility offers a valuable layer of resilience. However, in high-security environments ("Crypto Agility and Legacy Systems"), fixed cryptographic implementations may be preferred, as the flexibility introduced by crypto agility can also create new vulnerabilities.

Stimulating the Adoption of PQC

As discussed in the sections titled "Organizational" and "Incentives and Market Forces," significant barriers — including limited awareness, high migration costs and expertise shortages — currently hinder PQC adoption. The following recommendations directly respond to these identified gaps by providing targeted support through national strategies and initiatives.

Education, Training and Communication Initiatives

Incentives and Awareness i\Initiatives

A key barrier identified previously is the inconsistency of awareness regarding quantum computing risks across sectors ("Public-Private Awareness"). To bridge this gap, the Canadian government should implement a clear national communication strategy for industry leaders and cryptography professionals, outlining transition timelines and offering support to streamline migration. Such initiatives can address sectors less engaged with the quantum threat, such as health care, ensuring they understand the urgency of migration. Public sector awareness initiatives are essential, as government plays a dual role as both educator and enabler. Collaborations between industry and research groups, previously conveyed in "Communication Barriers," can increase participation and improve adoption preparedness.

In addition, to prevent misinformation and public panic associated with the quantum threat — issues documented in "Civilian Impact and Public Perception" — Canada's national PQC strategy should include a public communications campaign. As exemplified by the backlash against 5G technology, fear and misinformation can delay or derail the rollout of vital infrastructure. And as noted in recent academic analyses, Canada's evolving quantum posture reflects a shift toward securitization, with defence planning increasingly framing quantum technologies as strategic threats (Murphy and Parsons 2024). To counter this trend and promote democratic accountability, public engagement and transparent communication should be central to PQC migration strategies.

This campaign should provide accurate, accessible information to the public about quantum computing and PQC, clarifying what the quantum threat is, and is not. Public trust can be strengthened through media engagement, community briefings, and the inclusion of trusted voices from academia, government and industry. This effort could be led by the Cyber Centre, in partnership with ISED, ensuring clear and consistent messaging across platforms.

Centralized Resource for Technology Updates

As identified earlier ("Competing Narratives and Priorities"), industry leaders (for example, CIOs) face significant barriers balancing long-term quantum threats with immediate operational priorities. A centralized resource providing updates on quantum developments should be established.

Through the Cyber Centre, CSE serves as a central point of contact for organizations transitioning to PQC. As the migration process advances, available online public

information from CSE should be regularly updated to ensure organizations have access to necessary support and resources for effective PQC adoption. Current government communication regarding PQC is fragmented, making it harder for organizations to find the information and guidance they need to navigate the transition in a timely manner.

With the release of the NIST standards, CSE can expand and refine its existing guidance by clarifying the implications of these standards, outlining next steps for organizations and directing them to relevant, specific resources for further assistance. Strengthening these efforts will help organizations navigate the PQC transition more effectively and ensure a coordinated approach to implementation.

Start-Up Accelerators and PQC Adoption

The talent shortage discussed in "Resource Constraints" can be addressed through education and training initiatives. Programs supporting and mentoring early-stage and scale-up companies should incorporate education initiatives on the quantum threat, along with training and guidance on PQC adoption. This is particularly important for companies handling sensitive information, ensuring they are equipped to address quantum-related cybersecurity risks. Support should include directing these organizations to relevant resources on PQC adoption and key focus areas for early-stage start-ups, such as data security.

This approach includes allocating targeted resources to accelerators that support cybersecurity firms — particularly those developing PQC solutions compliant with NIST standards — to strengthen Canada's cryptographic security ecosystem. Strengthening this ecosystem will help ensure that start-up and scale-up firms are aware of the quantum threat and can take proactive measures to mitigate associated risks.

Training the Next Generation of Cryptographic Experts

One of the key challenges identified in "Resource Constraints" is the shortage of expertise available to support the transition to PQC. Addressing this gap requires investing in education and training to develop a new generation of cryptographic professionals. Some companies hire co-op students to nurture young talent, emphasizing the responsibility of experienced professionals to mentor and build the next generation of practitioners. Government policies that support businesses in hiring and training young professionals, such as subsidizing the costs of onboarding co-op students, play a critical role in expanding training opportunities, particularly for small companies.

Younger professionals are more adaptable and bring fresh perspectives to the field. Their ability to effectively manage context switching and embrace new challenges makes them well suited for tackling complex cryptographic problems. Collaboration between experienced professionals and emerging talent fosters innovation, ensuring the cryptographic field continues to evolve and effectively address future security challenges.

Partnership Programs

Public-private partnerships can play a crucial role in training talent and fostering innovation in PQC adoption. Subsidies from the public sector can provide financial support to accelerate progress and encourage collaboration between industry, academia and government.

Collaborative initiatives between the public and private sectors can help address

resource constraints by leveraging existing programs. For example, the Mitacs Accelerate fellowship trains graduate students and post-doctoral researchers across various disciplines, including quantum computing.[14] These researchers could contribute to projects for organizations such as the Bank of Canada, working under the joint supervision of an academic adviser and industry partners. Leveraging the Mitacs Accelerate fellowship for PQC implementation would offer support to organizations preparing for quantum-related threats.

Such initiatives not only bridge the gap between academic research and industry needs but also drive productivity growth by transforming specialized knowledge into practical applications. A professor, for example, could establish a spin-off company to provide cryptographic expertise and manage these transitions efficiently. Developing structured programs that connect experts, including technical project managers, with organizations would enhance the effectiveness of PQC implementation.

Financial and Resource Support for Transition

Government-Funded Tax Credits and Grants

The financial and resource constraints identified in "Leveraging Market Forces" present significant migration barriers, especially for SMEs and less-prepared sectors. To address this gap, government-funded initiatives can provide organizations with the necessary resources to facilitate system upgrades and prioritize data security during migration. Sectors handling sensitive information, such as health-care institutions and small financial entities such as credit unions, would particularly benefit from such support. The Canadian technology sector currently benefits from the Scientific Research and Experimental Development tax incentives, which encourage start-ups to engage in research and development within Canada.[15]

The National Research Council of Canada offers the Industrial Research Assistance Program (IRAP), which provides businesses with access to industrial technology advisers. These advisers offer technical and business guidance, referrals and support to help organizations transition from idea development to commercialization. Additionally, IRAP facilitates connections with regional, national and international partners, offering tailored support such as funding opportunities, market insights and expert advice to drive innovation and growth.[16]

Public-Sector Procurement Rules

The sections titled "Leveraging Market Forces" and "Informal Deterrents and Herd Behaviour" highlight the tendency of organizations to delay PQC adoption in the absence of clear market incentives or mandates. To accelerate migration, public-sector procurement rules should require PQC readiness as a condition of contract eligibility in sectors such as defence, health care and digital services (such policies should also include considerations of equity to ensure that smaller vendors, or those operated by under-represented groups, are not further disadvantaged).

This demand-side pressure, particularly when coordinated across jurisdictions, can normalize PQC as an industry expectation. In addition, governments can publish

14 See www.mitacs.ca/our-programs/accelerate-fellowship/.

15 See www.canada.ca/en/revenue-agency/services/scientific-research-experimental-development-tax-incentive-program.html.

16 See https://nrc.canada.ca/en/support-technology-innovation/nrc-irap-advisory-services.

implementation benchmarks, allowing market forces to encourage standardization and create competitive advantage for early adopters.

Ensuring Equity in Access to PQC Adoption

The section titled "Informal Deterrents and Herd Behaviour" raised concerns that PQC adoption might become stratified, where only well-resourced organizations can afford stronger cryptographic protections. To prevent the emergence of inequitable tiered-service models, financial support must be designed with equity as a core principle. Specifically, tax incentives and grants should be scaled to support SMEs, community-based institutions and non-profits, and critical service providers (for example, health care, credit unions) that handle sensitive information but lack technical capacity.

SMEs can also benefit from joining industry consortiums such as the Global Risk Institute (GRI), which provides insight into emerging risks and offers risk management support for the financial sector. GRI fosters collaboration among industry, academia and government by providing its members with educational resources, research publications and networking opportunities.[17]

Key Considerations for Evaluating Cryptographic Solutions for Implementation

To streamline decision making on PQC algorithm implementation, critical services can consider establishing blanket requirements for hybrid solutions to ensure a baseline level of security ("Crypto Agility and Legacy Systems"). Hybrid algorithms, which combine classical and quantum-resistant cryptographic methods, provide a smoother transition and reduce reliance on a single algorithm, increasing system diversity.

While these solutions are more data-intensive, costly and slower, they may serve as an effective interim measure for organizations that can accommodate them. However, hybrid algorithms are not always necessary, and selecting an appropriate cryptographic scheme requires cryptographic expertise. Organizations lacking such expertise may adopt hybrid solutions to ensure compliance and security.

NIST permits the hybrid approach if at least one cryptographic method is already NIST-approved and is updating its rules to support PQC algorithms in hybrid set-ups. This allows organizations to implement traditional PKC alongside PQC. When using two cryptographic methods, system security is only as strong as the most secure algorithm. If one method is compromised, the other should continue to protect the data.[18]

Decision-support tools can assist organizations in navigating PQC adoption. In the Netherlands, an open-source decision tool[19] provides compatibility scores for various algorithms. Governments can develop similar tools to help organizations assess which cryptographic scheme best suits their needs.

Widespread adoption of one of the three standardized PQC schemes offers advantages, improving interoperability between systems while diversifying the cryptographic landscape. Diversification strengthens resilience against potential algorithmic failures, enhancing the security and reliability of quantum-safe solutions.

17 See https://globalriskinstitute.org/about/.

18 See https://csrc.nist.gov/projects/post-quantum-cryptography/faqs.

19 See https://tno.github.io/PQChoiceAssistant/.

Canada's Leadership in Multilateral and Multi-Stakeholder Strategies

To address previously highlighted issues of fragmented regulatory frameworks and the lack of international alignment ("Global and Sovereignty Considerations" and "Interoperability and International Collaboration"), the following recommendations outline initiatives the government can implement to facilitate the effective adoption of PQC and ensure ongoing preparedness for emerging threats. This section examines the regulatory measures necessary to drive PQC adoption, future considerations for existing national strategies and opportunities for international collaboration to support a successful migration.

In Canada, CSE, through the Cyber Centre, is the technical authority on cryptography and is positioned to guide the country's transition to PQC. CSE can guide organizations through recommendations and guidelines, such as those in the United States that mandate migration deadlines. Sectors handling large volumes of sensitive data should have regulated PQC adoption deadlines to ensure they take the necessary precautions to maintain system security and protect their data.

Regulatory Measures

A phased approach to migration acknowledges the scale of the transition while emphasizing the urgency of mitigating quantum-related risks. Gaps in Canada's regulatory framework, including undefined migration timelines and a fragmented approach ("How Is Cryptography Currently Regulated in Canada?" and "Fragmented Governance and the Challenges of Coordinating PQC in Canada"), can hinder progress. Without a clearly defined starting date, transition end dates become less effective in guiding the migration process. To ensure an effective migration, both start and end dates must be established for major transitions.

Regulations should not only facilitate industry transitions but also prioritize public interest and consumer protection. Individual consumers, particularly in sectors such as telecommunications, rely on regulatory oversight to ensure that companies conduct due diligence in transitioning to PQC. Without clear regulations, everyday users would have little assurance that service providers are implementing necessary security measures.

Regulations play a crucial role in holding organizations accountable and safeguarding public trust. Since different sectors have varying security requirements, regulations should be designed to match their specific needs, ensuring that the level of security is appropriate for the sensitivity of the data they handle. As outlined in the sections titled "How Is Cryptography Currently Regulated in Canada?" and "Fragmented Governance and the Challenges of Coordinating PQC in Canada," which discuss how cryptography is regulated in Canada and compare the regulatory frameworks of Canada and the United States, PQC migration will require coordination across multiple government agencies, including the CSE, ISED and OSFI, among others.

Governments are uniquely positioned to establish standards and certification processes that ensure public safety and security. These mechanisms include certifying cryptographic tools and mandating their adoption across critical industries.

Regulatory frameworks can define migration timelines earlier in the transition process. The United States provides a relevant example, having set a 2035 deadline

for PQC adoption. However, the timeline for actual quantum threats remains uncertain (CISA 2024). Security should be approached as an ongoing process of preparation for potential unknown risks, rather than as a response to specific threats once they materialize.

As previously discussed, Canada's regulatory approach is shaped by its close economic and technological ties with the United States and its adequacy status under PIPEDA (see Appendix 4 for more details). This compliance framework enables Canadian products to align with privacy laws in both the United States and Europe.

Key Factors to Consider for National Strategies

Continuous Adaptation for Quantum Threat Migration

Ongoing efforts are essential to understanding and addressing the evolving risks posed by quantum technologies ("Risk Timelines and Technology Life Cycle" and "Urgency and Timelines"). As advancements in quantum computing continue, states, private sector actors and other stakeholders must remain vigilant, focusing on both immediate risks and the long-term implications of these developments. Effective risk mitigation requires sustained collaboration among stakeholders.

As quantum computing advances, migration plans should be updated regularly to keep up with the evolving threat. While progress has been made in recognizing quantum threats and advancing quantum technologies, continuous efforts are needed to address emerging challenges. Planning and strategizing cannot end with the release of national strategies, such as quantum or cybersecurity initiatives. Instead, these efforts must be part of an ongoing process to anticipate threats over the coming years and foster cooperation among states and other stakeholders to mitigate both current and future risks.

Expert insights reinforce the need for continuous adaptation. As quantum computing progresses, so must the strategies and collaborations designed to address its risks. Stakeholders across sectors need to regularly reassess and refine their strategies to ensure long-term security. This continuous approach will not only mitigate immediate threats but also establish a strong foundation for managing future challenges in the quantum landscape.

Global Efforts for Migration

Global Quantum-Safe Fora

Securing against the quantum threat to cryptography requires international collaboration ("Interoperability and International Collaboration"). Consultations can be organized to bring together participants from global industries and governments. These discussions should include representatives from organizations such as the International Telecommunication Union (ITU), ISO, the Institute of Electrical and Electronics Engineers, ETSI, NIST and industry developing security applications, appliances and devices. Establishing these conversations early is essential to ensuring global coordination. A global quantum-safe forum could serve as a dedicated platform for these discussions. Currently, these efforts remain fragmented and lack a cohesive international framework. The development of mature technologies, such as cellular networks, demonstrates how effective collaboration between governments, industry and academia can lead to alignment when all stakeholders engage in structured dialogue.

Canada's NQS and associated policy documents emphasize international alignment as a core objective. This is echoed in assessments of the DND/CAF Quantum 2030 plan, which identify global coordination, particularly through the North Atlantic Treaty Organization's Defence Innovation Accelerator for the North Atlantic and the G7, as vital to quantum readiness (DND/CAF 2023). These fora offer opportunities to develop standards, coordinate migration timelines and support multilateral security cooperation.

Diversifying Regulatory Engagement

While Canada has historically aligned with US cybersecurity standards (see "Geopolitical Dynamics and the Impact on Standardization"), recent geopolitical instability and sovereignty concerns ("Global and Sovereignty Considerations") suggest the need for a more diversified regulatory strategy. To mitigate overreliance on a single partner, Canada can deepen its engagement with European and multilateral standardization bodies and align PQC implementation with global regulatory frameworks such as the GDPR. This approach will not only preserve Canada's adequacy status under GDPR but also future-proof Canadian exports and increase global market compatibility.

Regular Meetings for Policy Makers

To maintain ongoing alignment, regulators and policy makers should convene regularly to stay informed on international standards and coordinate their efforts. A relevant example is a 5G round table hosted in Ottawa, where network manufacturers participated alongside standards bodies such as ETSI and ITU. Hosting similar round tables for PQC would integrate industry players into discussions with standards bodies, fostering collaboration and ensuring alignment.

These fora and meetings could feature program committees responsible for organizing presentations and facilitating knowledge exchange. Industry representatives would provide strategic direction, while standards bodies would clarify technical limitations, ensuring that innovation aligns with regulatory frameworks. Canada can take a leadership role in hosting these discussions on PQC standards and best practices, leveraging its commitment to interoperability as a foundation for global cooperation.

Appendix 1: Research Methodology

The advent of quantum computers poses significant risks to our digital security, given their ability to break existing cryptographic schemes. Transitioning to PQC is essential for securing our digital infrastructure and protecting sensitive data. Given the security threats posed by quantum computing, migrating our systems to PQC is both crucial and time critical. Work on the development and standardization of PQC algorithms is being pursued by both the private and public sectors worldwide, with NIST taking the lead. Although NIST has initiated the process of standardizing PQC algorithms, these guidelines are non-enforceable, especially in the private sector. This study investigated whether the transition to PQC should be regulated and led by the public sector or driven by the free market. The authors aimed to investigate three

main research questions to understand how Canada is currently approaching the transition to PQC, and how it should continue to do so:

- Should the transition to PQC be solely regulated by the government, or should it be driven voluntarily by the free market?
- How effective are voluntary compliance measures compared to regulations enforced by the government when ensuring the successful adoption of PQC?
- What are the implications of the various regulatory and market-driven approaches on the standardization, regulation, technological adoption pace and impact on critical infrastructure in Canada?

Existing research highlights the importance of transitioning to PQC for the security and integrity of data against quantum computers. Private sector organizations such as SandboxAQ (a spinoff from Alphabet Inc.) have investigated potential timelines and strategies for transitioning cryptographic systems to PQC to protect digital systems against the quantum threat (Joseph et al. 2022). Meanwhile, institutions such as the Belfer Center for Science and International Affairs at the Harvard Kennedy School (Trzcinski et al. 2023) and the Delft University of Technology (Kong, Janssen and Bharosa 2024) have examined the governance and implementation of PQC from a policy perspective.

The intersection of quantum information science and public policy is an emerging field, and, as such, there are limited peer-reviewed sources available. The authors have tried to corroborate their evidence, seeking support from industry, academic and government perspectives to support their claims.

Data Collection

This policy analysis draws on existing policy reports, literature and qualitative interviews with subject experts. Over the course of the study, the authors conducted 19 interviews with experts in academia and the public and private sectors. Participants were anonymized to ensure confidentiality and to facilitate open dialogue during interviews.

The authors' inclusion criteria for the qualitative interviews were individuals with expertise in addressing the regulatory challenges of PQC. The selection process was based on the knowledge and expertise of the two co-principal investigators in the field of quantum computing. The interviewees included experts in technology policy and standards development, mathematicians researching PQC, private sector leaders and public servants engaged in PQC or broader quantum technology initiatives.

Data Analysis

The qualitative interviews included a list of 12 prepared questions covering the quantum-safe transition, regulatory frameworks, implementation challenges as well as the role of the public and private sectors. The list of interview participants is included in Table 1. The interviews were recorded and transcribed by Microsoft Teams. Based on the data collected from the interviews, the authors conducted thematic analysis on the transcripts, identifying key themes emerging from the conversations. The authors followed the guidelines as outlined by the Research Ethics Board to anonymize the data, and any information related to the participants.

Appendix 2: Certification and Testing Processes

The Cryptographic Algorithm Validation Program (CAVP) is a framework established by NIST to ensure cryptographic algorithms and their individual components meet specific security standards. It focuses on validating cryptographic algorithms that are FIPS-approved or NIST-recommended. The program is an important step for achieving cryptographic module certification under the FIPS 140 program, which is a standard for assessing and certifying cryptographic products used by government agencies and industries.

The program ensures a streamlined validation process by using NVLAP-accredited cryptographic- and security-testing laboratories, which handle the technical evaluation of cryptographic

Table 4: Comparison of Cryptographic Algorithm and Module Validation Processes

	Cryptographic Algorithm Validation	Cryptographic Module Validation
Focus	Algorithm functionality and security	Entire module security, including algorithms
Scope	Single algorithm implementation	Complete cryptographic system
Program	CAVP	CMVP
Standards	N/A	FIPS 140-2 or FIPS 140-3
Outcome	Validates algorithm for potential use	Certifies module for secure deployment

Source: Authors; see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program; https://csrc.nist.gov/Projects/cryptographic-module-validation-program; https://csrc.nist.gov/glossary/term/cryptographicmodule.

algorithms. These laboratories leverage the Automated Cryptographic Validation Testing System to create test cases that align with the specific capabilities of the algorithm being evaluated. Once the algorithm processes the test inputs, the system determines whether the outputs meet the required standards. Algorithms that pass are added to a validation list, which includes information about the vendor, operational environment and specific attributes of the validated algorithm. [20]

Cryptographic algorithm validation is a required step before cryptographic module validation. The CMVP is run by NIST and the Cyber Centre to ensure cryptographic modules meet the set of testable cryptographic and security requirements. Validated modules are placed on an active list for five years, and they can be applied to new and existing systems; however, interim validated modules are on the active

20 See https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program.

list for two years.[21] Cryptographic modules include the hardware and software that implement the cryptographic algorithms along with other approved security functions.[22] The differences between the two are highlighted in Table 1.

While the Cyber Centre does not enforce the use of specific algorithms, such as RSA or Advanced Encryption Standard, it strongly recommends using certified standard cryptography to avoid vulnerabilities that stem from errors in implementation. These certification mechanisms validate cryptographic systems, helping organizations identify potential mistakes that could lead to security weaknesses.

For certain classified information, the Cyber Centre acts as an authority within the Government of Canada, setting specific rules and policies that departments must follow. However, its influence over private sector organizations remains limited to guidance rather than mandates. Unlike NIST in the United States, which has the authority to require certain cryptographic standards for specific agencies, the Cyber Centre primarily provides recommendations. The enforcement of policies within Canadian government departments, when required, falls under the jurisdiction of the TBS. This collaborative framework ensures that cryptographic standards are aligned across Canadian government entities while offering best practices to the broader public and private sectors.

Appendix 3: Government Cryptographic Standards and Security Policies

This appendix offers an overview of the documents outlining guidelines and standards established by the TBS and CSE. It provides additional details about the standards referenced in the main text, including explanations of the responsible governing bodies and their respective roles. The document titled "Cryptographic algorithms for Unclassified, Protected A, and Protected B information" was first released in August 2016 and was last updated in March 2024 (The Cyber Centre 2024). There have been no updates since the release of the NIST PQC standards in August 2024. It mainly contains information on cryptographic algorithms, key establishment and digital signature schemes, to list a few of the specific cryptography-related topics. However, this document was released by the Cyber Centre and is meant for evaluating and providing guidance on cryptographic algorithms for unclassified information within government departments (ibid.). The document is intended to add to information shared by the Government of Canada in the "Guideline on Defining Authentication Requirements," which outlines more information on risk assessment and evaluating how to best secure its data and systems in a way that fits the government's needs (Government of Canada 2012). The guideline is designed to help government departments and agencies establish clear authentication (identity verification) requirements for their programs and services. Essentially, it provides a framework for ensuring secure and compliant identity verification in service delivery (ibid.). The document falls under the Directive on Identity Management, part of the Policy on Government Security.

21 See https://csrc.nist.gov/Projects/cryptographic-module-validation-program.

22 See https://csrc.nist.gov/glossary/term/cryptographicmodule.

The policy falls under the Foundation Framework for Treasury Board Policies, which provides an overview of how Treasury Board policy instruments are organized and highlights the general requirements that apply to all Treasury Board policy instruments (TBS 2008). The policy is designed to ensure that security measures in the Government of Canada are effectively managed to protect security information and people. It outlines the roles and responsibilities of deputy heads, deputy heads of internal enterprise service organizations, deputy heads of lead security agencies and the Secretary of the Treasury Board in managing security within the Government of Canada. A few of the responsibilities described for the deputy heads include establishing a governance framework for managing security controls and risk decisions, approving a three-year security plan that is updated annually, and coordinating government-wide actions by responding to requests from the TBS or the Privy Council for coordinated security responses.

The policy also identifies key government organizations and their roles in supporting the Government of Canada's security policy objectives. This list includes CSE, which is responsible for addressing cyberthreats and is the national authority for cryptographic intelligence. Public Safety Canada is responsible for taking the lead in organizing efforts related to national security and cybersecurity, including coordinating strategies among various government departments to address security threats and challenges at a national level. Public Services and Procurement Canada is responsible for providing and managing secure IT systems used across various government departments. Shared Services Canada is responsible for planning, designing, implementing, operating and maintaining IT security infrastructure for the Government of Canada.

Under the Policy on Government Security (Government of Canada 2019a) are two directives: the "Directive on Identity Management" and the "Directive on Security Management" (Government of Canada 2019b). The latter describes the roles and responsibilities of various individuals and groups within the Canadian government departments in managing, maintaining and enforcing security in accordance with the Policy on Government Security. It outlines the hierarchy of security responsibilities and provides a framework to ensure accountability and collaboration in government security practices (ibid.).

Appendix 2 on "Mandatory Procedures for Information Technology Security Screening Control" outlines expectations for managing IT security in government. The procedures are in line with what experts have explained are important cybersecurity practices in the migration to PQC. These procedures include defining and maintaining IT security requirements for systems by identifying threats to protect throughout the system's life cycle. This also includes considering security requirements throughout the system's life cycle as well as addressing supply chain risks, to name a few.

While the Cyber Centre document on cryptographic algorithms for unclassified information provides in-depth information relating to cryptographic algorithms for organizations, the TBS document specifying the "Guideline on Defining Authentication Requirements" provides information to allow organizations to first assess their systems and identify risks (Government of Canada 2012).

These documents and policies describe the guidelines and best practices for the federal government. Provincial governments have a separate set of cryptographic standards. For instance, the Government of Ontario Information and Technology Standards 25.12 outlines security requirements for the use of cryptography within the Government of Ontario (2025). These standards outline responsibilities within the Government of

Ontario, including for cryptographic service providers to the provincial government that ensure the secure operation of cryptographic systems. The cybersecurity division within the Ontario government oversees the creation, implementation and assessment of cybersecurity policies and cryptographic systems for government. It manages the PKI for the Ontario Public Service, monitoring advancements in technology to evaluate strengths, vulnerabilities and appropriate cryptographic solutions. The cybersecurity division also ensures compliance with security standards and collaborates with other levels of government to coordinate cryptographic practices. The Ontario Internal Audit Division also plays a key role in maintaining compliance with security standards by conducting regular audits of cryptographic and security activities (ibid.).

Appendix 4: Additional Resources on PIPEDA

Office of the Privacy Commissioner of Canada

This website provides an overview of PIPEDA.[23] It outlines key responsibilities for organizations handling personal data, including the 10 fair information principles, sector-specific regulations and how PIPEDA applies across different jurisdictions. There is also information regarding provincial privacy laws, federally regulated organizations and cross-border data protection requirements.

PIPEDA

This website provides the full text of PIPEDA.[24] It includes official legal definitions, regulatory provisions and compliance requirements related to privacy protection in the private sector. This also outlines application criteria, enforcement mechanisms and sector-specific privacy obligations under Canadian law.

EU Adequacy Decisions

The European Commission provides information on the European Union's adequacy decisions[25] under article 45 of the GDPR. It explains how the European Union determines whether a non-EU country offers an adequate level of data protection, allowing data to flow freely without additional safeguards. There is also information on the evaluation process, periodic reviews and recent adequacy decisions, as well as updates on international data protection agreements.

23 See www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

24 See https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html.

25 See https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Canada's PIPEDA and EU Adequacy Status: Implications for Cross-Border Data Flows

This Centre for International Governance Innovation opinion piece discusses the European Commission's adequacy decision on Canada's data protection framework under the GDPR (Bennett 2024). It explains how Canada's PIPEDA remains compliant with EU data protection standards, allowing continued cross-border data flows.

Appendix 5: Terminology

Certificate authority: An established authority that validates public keys by issuing and revoking digital certificates used to confirm identity and ensure secure communication.[26]

CRQC: A quantum computer capable of compromising existing public-key cryptographic algorithms (The White House 2022b).

Digital signatures: The output of a cryptographic process that ensures the authenticity of the source, verifies the integrity of the data and provides evidence that the signer cannot deny their involvement (Barker, Roginsky and Davis 2020).

Digital trust: The confidence individuals have that digital technologies, services and the organizations behind them will safeguard stakeholder interests and adhere to societal values and expectations.[27]

Legacy systems: An outdated but essential information system that supports daily operations. One of the biggest challenges for IT professionals is replacing these systems with modern technologies while ensuring compatibility with existing systems and data formats still in use as organizations upgrade or transition their infrastructure.[28]

OT: Systems and devices that regulate or respond to changes in the physical environment by monitoring, managing and controlling processes and events. These technologies are commonly used in industrial automation, building management, fire safety and access control systems.[29]

PKC: A cryptographic system that utilizes a pair of public and private keys for encrypting data and verifying digital signatures.[30]

PKI: The framework and operational processes that govern the use of certificate-based PKC, including issuing, maintaining and revoking public-key certificates.[31]

26 See https://csrc.nist.gov/glossary/term/certificate_authority.

27 See https://initiatives.weforum.org/digital-trust/home.

28 See www.gartner.com/en/information-technology/glossary/legacy-application-or-system.

29 See https://csrc.nist.gov/glossary/term/operational_technology.

30 See https://csrc.nist.gov/glossary/term/public_key_cryptography.

31 See https://csrc.nist.gov/glossary/term/public_key_infrastructure.

PQC: Cryptographic algorithms designed to withstand attacks from both classical and quantum computers, ensuring data security in the era of CRQCs. It is also referred to as QSC and QRC.[32]

SNDL: This refers to the interception and storage of encrypted data by threat actors today, with the aim of decrypting it in the future once a quantum computer capable of breaking current cryptographic standards is developed. This poses a long-term risk to sensitive information, particularly in sectors where data must remain confidential over the long term, such as national security, health care and critical infrastructure. This threat is also known as "harvest now, decrypt later" (The Cyber Centre 2025b).

SSH certificate: A type of digital credential used to securely confirm a person's identity when accessing computer systems through SSH. Instead of granting access with individual security keys for each person, an SSH certificate is issued and approved by a trusted source called a certificate authority. This helps organizations manage who can access their systems in a more efficient and secure way.[33]

TLS: A well-established protocol used to enable encrypted communication across networks, particularly on the web. It secures data transmission by applying various cryptographic techniques to protect the integrity and confidentiality of information exchanged between systems.[34]

32 See https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/FAQ/index.html.

33 See https://docs.github.com/enterprise-cloud@latest/organizations/managing-git-access-to-your-organizations-repositories/about-ssh-certificate-authorities.

34 See www.ibm.com/docs/en/sdk-java-technology/8?topic=provider-tls-protocol-overview.

Works Cited

Auer, Raphael, Donna Dodson, Angela Dupont, Maryam Haghighi, Nicolas Margaine, Danica Marsden, Sarah McCarthy and Andras Valko. 2025. "Quantum-readiness for the financial system: a roadmap." BIS Paper No. 158. July. www.bis.org/publ/bppdf/bispap158.pdf.

Barker, Elaine, Allen Roginsky and Richard Davis. 2020. "Recommendation for Cryptographic Key Generation." NIST Special Publication 800-133, Revision 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf.

Bennett, Colin J. 2024. "The 'Adequacy' Test: Canada's Privacy Protection Regime Passes, but the Exam Is Still On." Opinion, Centre for International Governance Innovation, April 3. www.cigionline.org/articles/the-adequacy-test-canadas-privacy-protection-regime-passes-but-the-exam-is-still-on/.

Campagna, Matthew, Lidong Chen, Özgür Dagdelen, Jintai Ding, Jennifer K. Fernick, Nicolas Gisin, Donald Hayford et al. 2015. *Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges*. ETSI White Paper No. 8. June. www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

———. 2025a. "Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)." Ottawa, ON: CSE. www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001.

———. 2025b. "Preparing your organization for the quantum threat to cryptography (ITSAP.00.017)." February. www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017.

Chen, Lily and Matthew Scholl. 2022. "The Cornerstone of Cybersecurity – Cryptographic Standards and a 50-Year Evolution." *Cybersecurity Insights* (NIST blog), May 26. www.nist.gov/blogs/cybersecurity-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution.

CISA. 2024. "Strategy for Migrating to Automated Post-Quantum Discovery and Inventory Tools." August 15. www.cisa.gov/sites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf.

De Luca, Stefano. 2024. "Cryptographic security: Critical to Europe's digital sovereignty." European Parliamentary Research Service Briefing PE 766.237. November. www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf.

Denholm, Paul, Trieu Mai, Rick Wallace Kenyon, Ben Kroposki and Mark O'Malley. 2020. *Inertia and the Power Grid: A Guide Without the Spin*. National Renewable Energy Laboratory Technical Report NREL/TP-6A20-73856. May. www.nrel.gov/docs/fy20osti/73856.pdf.

Deodoro, Jose, Michael Gorbanyov, Majid Malaika and Tahsin Saadi Sedik. 2021. "Quantum Computing and the Financial System: Spooky Action at a Distance?" International Monetary Fund Working Paper WP/21/71. www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159.

DND. 2025. "Canada's new government is rebuilding, rearming, and reinvesting in the Canadian Armed Forces." Press release, June 9. www.canada.ca/en/department-national-defence/news/2025/06/canadas-new-government-is-rebuilding-rearming-and-reinvesting-in-the-canadian-armed-forces.html.

DND/CAF. 2023. *Quantum 30: The Department of National Defence and Canadian Armed Forces Quantum Science & Technology Strategy Implementation Plan*. Ottawa, ON: Government of Canada. www.canada.ca/en/department-national-defence/corporate/reports-publications/overview-quantum-2030/quantum-s-t-strategy-implementation-plan.html.

European Commission. 2024. “Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography.” C(2024) 2393 final. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.`

Forrest, Tracey and Michael P. A. Murphy. 2025. “Vision for the Future of Quantum Technologies: Survey Results.” Waterloo, ON: CIGI. www.cigionline.org/static/documents/Quantum-survey.pdf.

G7 Finance Ministers and Central Bank Governors. 2025. “G7 Finance Ministers and Central Bank Governors’ Communiqué.” May 20. https://g7.canada.ca/en/news-and-media/news/g7-finance-ministers-central-bank-governors-communique/.

G7 Leaders. 2025. “Kananaskis Common Vision for the Future of Quantum Technologies.” G7 Leaders’ Statement, June 17. https://g7.canada.ca/en/news-and-media/news/kananaskis-common-vision-for-the-future-of-quantum-technologies/.

GAO. 2024. “Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy.” GAO-25-107703. November 21. www.gao.gov/assets/gao-25-107703.pdf.

Gidney, Craig. 2025. “How to factor 2048 bit RSA integers with less than a million noisy qubits.” *arXiv*, June 9. https://doi.org/10.48550/arXiv.2505.15917.

Government of Canada. 2012. “Guideline on Defining Authentication Requirements.” November 30. www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=26262.

———. 2019a. “Policy on Government Security.” July 1. www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578.

———. 2019b. “Directive on Security Management.” July 1. www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611.

Government of Ontario. 2025. “GO-ITS 25.12 Security Requirements for the Use of Cryptography.” Toronto, ON: Government of Ontario. www.ontario.ca/page/go-its-2512-use-cryptography.

Herman, Arthur and Alexander Butler. 2023. *Prosperity at Risk: The Quantum Computer Threat to the US Financial System*. April. Washington, DC: Hudson Institute. www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system.

ISED. 2022. *Canada’s National Quantum Strategy*. Ottawa, ON: ISED. https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy.

———. 2025. *National Quantum Strategy Roadmap: Quantum Communication and Post-Quantum Cryptography*. February 17. Ottawa, ON: ISED. https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography.

Joseph, David, Rafael Misoczki, Mark Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer et al. 2022. “Transitioning organizations to post-quantum cryptography.” *Nature* 605: 237–43. https://doi.org.10.1038/s41586-022-04623-2.

Kong, Ini, Marijn Janssen and Nitesh Bharosa. 2024. “Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions.” *Government Information Quarterly* 41 (1): 101884. https://doi.org/10.1016/j.giq.2023.101884

Leech, David P. and Michael W. Chinworth. 2001. *Planning Report 01-2: The Economic Impacts of NIST’s Data Encryption Standard (DES) Program*. October. Arlington, VA: TASC. www.nist.gov/system/files/documents/2017/05/09/report01-2.pdf.

Meijaard, Yoram, Dayana Spagnuelo and Nitesh Bharosa. 2023. *Application of the societal risk assessment method*. HAPKIDO Deliverable 1.2. https://hapkido.tno.nl/publish/pages/4065/20231008_hapkido_deliverable_1-2_application_of_the_sra_method_final_report.pdf.

Mosca, Michele and John Mulholland. 2017. *A Methodology for Quantum Risk Assessment*. January 5. Toronto, ON: GRI. https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/.

Mosca, Michele and Marco Piani. 2019. *Quantum Threat Timeline Report*. October 3. Toronto, ON: GRI. https://globalriskinstitute.org/publication/quantum-threat-timeline/.

———. 2021. *Quantum Threat Timeline Report 2020*. January. GRI and evolutionQ. https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2020/.

Murphy, P. A. and Claire Parsons. 2024. "Tracking Quantum S&T from strategy to implementation plan: what we learned about the Canadian Armed Forces' quantum posture." *Canadian Foreign Policy Journal* 30 (3): 264–79. https://doi.org/10.1080/11926422.2024.2387209.

———. 2025. "Overcoming Securitization in Quantum Science and Technology Policy." Centre for International and Defence Policy, February 10. www.queensu.ca/cidp/overcoming-securitization-quantum-science-and-technology-policy.

National Cyber Security Centre. 2024. "Post-quantum cryptography." In *NCSC Annual Review 2024*, 68–71. www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-04/post-quantum-cryptography.

———. 2025. "Timelines for migration to post-quantum cryptography." March 20. www.ncsc.gov.uk/guidance/pqc-migration-timelines.

NIS Cooperation Group. 2025. "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography." Part 1. June 11. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

NIST. 2019. "Security Requirements for Cryptographic Modules." FIPS Pub 140- 3. March 22. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

———. 2022. "NIST PQC License Summary and Excerpts." https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/selected-algos-2022/nist-pqc-license-summary-and-excerpts.pdf.

———. 2023. "NIST Publishes Guide to Operational Technology (OT) Security." News release, September 28. www.nist.gov/news-events/news/2023/09/nist-publishes-guide-operational-technology-ot-security.

———. 2024. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." News release, August 13 (updated February 4, 2025). www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

NSA. 2022. "The Commercial National Security Algorithm Suite 2.0. and Quantum Computing FAQ." Cybersecurity Information Sheet. Version 2.1. December. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF.

OSFI. 2022. "Technology and Cyber Risk Management." Guideline No. B-13. July 31. www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management.

Parker, Edward. 2025. "U.S.-Allied Militaries Must Prepare for the Quantum Threat to Cryptography." Just Security, May 28. www.justsecurity.org/113733/quantum-computing-crytopography/.

Prime Minister of Canada. 2025. "Joint Statement: Enduring Partnership, Ambitious Agenda." June 23. www.pm.gc.ca/en/news/statements/2025/06/23/joint-statement-enduring-partnership.

Ratnam, Elizabeth L., Kenneth G. H. Baldwin, Pierluigi Mancarella, Mark Howden and Lesley Seebeck. 2020. "Electricity system resilience in a world of increased climate change and cybersecurity risk." *The Electricity Journal* 33 (9): 106833. https://doi.org/10.1016/j.tej.2020.106833.

TBS. 2008. "Foundation Framework for Treasury Board Policies." June 24. www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=13616.

The Cyber Centre. 2024. "Cryptographic algorithms for Unclassified, Protected A, and Protected B information." ITSP.40.111. March 5. Ottawa, ON: CSE. www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111#b13.

The White House. 2022a. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." Statements and Releases, May 4. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

———. 2022b. "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." Statements and Releases, May 4. https://irp.fas.org/offdocs/nsm/nsm-10.pdf.

Trzcinski, Andrew, Sreya Vaidyanathan, Ariel Higuchi and Amritha Jayanti. 2023. "Post-Quantum Cryptography." Technology Primers for Policymakers Series. Technology and Public Purpose Project. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. www.belfercenter.org/publication/technology-primer-post-quantum-cryptography.

Vermeer, Michael J. D., Chad Heitzenrater, Edward Parker, Alvin Moon, Domenique Lumpkin, Jalal Awan and Patricia A. Stapleton. 2023. *Evaluating Cryptographic Vulnerabilities Created by Quantum Computing in Industrial Control Systems*. Homeland Security Operational Analysis Center operated by the RAND Corporation Research Report RRA2427-1. October 4. www.rand.org/pubs/research_reports/RRA2427-1.html.

Vermeer, Michael J. D., Edward Parker and Ajay K. Kochhar. 2022. *Preparing for Post-Quantum Critical Infrastructure: Assessments of Quantum Computing Vulnerabilities of National Critical Functions*. Homeland Security Operational Analysis Center operated by the RAND Corporation. August 18. www.rand.org/pubs/research_reports/RRA1367-6.html.

World Intellectual Property Organization. 2014. "Patent Pools and Antitrust – A Comparative Analysis." March. www.wipo.int/documents/743993/747687/patent_pools_report.pdf.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org