Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)

ITSM

Canada

Foreword

This is an UNCLASSIFIED publication, issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information or to suggest amendments, contact the Cyber Centre:

- by email: cryptography-cryptographie@cyber.gc.ca
- by phone: 613-949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on June 23, 2025.

Revision history

Revision	Amendments	Date
1	First release.	June 23, 2025

ISBN 978-0-660-77914-0
CAT D97-4/40-001-2025E-PDF

Overview

Every organization managing information technology (IT) systems must migrate cyber security components to become quantum-safe. This will help protect against the cryptographic threat of a future quantum computer. The Cyber Centre recommends the adoption of standardized post-quantum cryptography (PQC) to mitigate this threat.

This publication outlines the Cyber Centre's recommended roadmap for the Government of Canada (GC) to migrate non-classified IT systems[1] to use PQC, including milestones, deliverables, and guidance for departmental planning and execution.

Milestones and deliverables for federal departments and agencies are as follows:

- April 2026: Develop an initial departmental PQC migration plan
- Beginning April 2026 and annually after: Report on PQC migration progress
- End of 2031: Completion of PQC migration of high priority systems
- End of 2035: Completion of PQC migration of remaining systems

[1] Non-classified IT systems are those that do not contain, transfer, or otherwise handle classified information. In the Government of Canada, non-classified systems manage UNCLASSIFIED, PROTECTED A, and PROTECTED B information. For classified systems and systems handling PROTECTED C information, departments must contact the Cyber Centre to obtain advice on migrating commercial equipment.

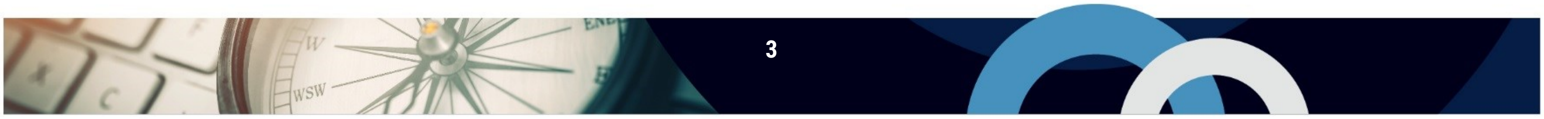


Table of contents

1 Introduction

The Cyber Centre recommends organizations managing IT systems migrate to use PQC in order to replace public-key cryptography vulnerable to a future quantum computer.[2] All instances of public-key cryptography must be migrated to secure GC IT systems and Canadians' data against this threat.

The United States' National Institute of Standards and Technology (NIST) has worked globally with cryptographic experts to standardize PQC algorithms that can replace existing vulnerable public-key cryptography. Cyber Centre recommendations for PQC algorithms are provided in Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP 40.111). As standards for network security protocols support PQC algorithms, the Cyber Centre will update the Guidance on securely configuring network protocols (ITSP.40.062) publication. Vendors are incorporating PQC in their products to rapidly meet the needs of government and industry.

The PQC migration within the GC will require significant commitment and take several years. The Cyber Centre is working with Treasury Board of Canada Secretariat (TBS) and Shared Services Canada (SSC) to prepare necessary updates to GC guidance, support and policy. Departments will need to clearly understand their cryptography usage. IT infrastructure, both hardware and software, and data will need to be analyzed across the entire enterprise. Starting the PQC migration early is important to leverage existing IT lifecycle budgets as much as possible.

This publication is the Cyber Centre's recommended roadmap for the migration of non-classified IT systems within the GC to use PQC. It outlines the stakeholders, execution phases, milestones and governance involved in this GC-wide cyber security activity. The intention is to provide key activities and timelines that will assist in coordination of departmental planning activities for migrating to PQC across the GC. It is aimed at directors and managers of IT systems in federal departments and agencies and decision makers accountable for the migration to PQC.

[2] For more information on the quantum computing threat to cryptography, read the publication Preparing your organization for the quantum threat to cryptography (ITSAP.00.017): https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

2 Stakeholders and planning

The Cyber Centre is the lead technical authority for information technology (IT) security in the GC.[3] As part of Canada's cryptologic agency, the Communications Security Establishment Canada, the Cyber Centre:

- promotes awareness of the quantum computing threat to cryptography to GC departments
- provides guidance on cryptographic recommendations, such as the use of PQC
- provides recommendations on incorporating cryptography into a strong cyber security posture

The Cyber Centre will continue to provide relevant advice and guidance to support GC departments and agencies in the migration to PQC.

TBS is responsible for establishing and overseeing a whole-of-government approach to security management, including cyber security, through policy leadership, strategic direction, and oversight. In May 2024, TBS published the Government of Canada's Enterprise Cyber Security Strategy identifying a key action to transition GC systems to use standardized PQC to protect GC information and assets from the quantum threat. TBS will issue the necessary policy instruments to require responsible officials to establish a departmental PQC migration plan as well as report on progress under existing departmental reporting processes.

SSC manages IT infrastructure and services on behalf of many of the departments and agencies across the GC. Due to its critical role in modernizing GC systems, SSC is already engaged in developing a plan for the migration to PQC and is working directly with the Cyber Centre and TBS to advise on the feasibility of implementation.

Federal departments and agencies in the GC are accountable for managing cyber security risks in their program areas. Departments and agencies will be responsible for maintaining software hosted on SSC-managed IT infrastructure, and any IT infrastructure that is managed separately from SSC, including contracted cloud services. Departments and agencies will be required to develop a tailored departmental PQC migration plan that covers the migration of systems for which they are responsible to use PQC. Departments and agencies will be responsible for executing that plan, as well as tracking and reporting on progress. This publication contains the initial considerations that can be used to develop a departmental PQC migration plan, but additional guidance and support will be provided by TBS, SSC and the Cyber Centre.

[3] Treasury Board Secretariat of Canada's Policy on Government Security: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578

3 Execution phases

This roadmap outlines 3 recommended phases to implement the PQC migration. These phases will likely overlap.

3.1 Preparation

During the preparation phase, departments and agencies will be responsible for developing a departmental PQC migration plan to migrate systems for which they are responsible to use PQC. To develop this plan, we recommend establishing a committee and identify a dedicated migration lead. The committee should consist of stakeholders throughout the organization and should include at least one member from senior management to ensure executive buy in and support. In addition to technical areas responsible for managing IT systems, we recommend the inclusion of stakeholders from non-technical areas such as finance, project management, procurement and asset management.

The departmental PQC migration plan needs to be continually revised and expanded upon during the execution of the subsequent phases. The initial version of the departmental PQC migration plan should establish the individuals responsible for the following:

- execution of the plan
- financial planning
- education strategy to inform staff on the quantum threat and the progress of this migration within the organization
- procurement policies for new equipment
- approaches for the identification of vulnerable systems to build an inventory for transition

3.1.1 Roles and responsibilities

The departmental PQC migration plan must identify individuals responsible for various tasks in the execution of the plan. Ultimately, the Designated Official for Cyber Security (DOCS) is accountable for mitigating the quantum risk to cyber security. We recommend the DOCS, or a delegated executive official, be assigned the role of PQC Migration Executive Lead to provide:

- oversight
- accountability
- executive support for the execution of the departmental PQC migration plan

The coordination and cross-departmental engagement may be performed by a PQC Migration Technical Lead. The Technical Lead would be responsible for facilitating coordination across the organization which may include service delivery, network management and IT procurement, as well as other areas pertinent to the migration. The committee established to develop the departmental PQC migration plan may be repurposed for managing the execution of the plan.

3.1.2 Financial planning

Departments and agencies should expect that many existing IT systems may need to be replaced, or new service contracts put into place to support PQC. The execution of the PQC migration will have staffing impacts that may require new hiring, external contractors, or the realignment of roles that could affect other projects or work activities. The departmental PQC migration plan must have a cost estimate that includes resource allocation to complete the execution. The initial version of plan will not be comprehensive in its cost estimation, but the financial estimates can be refined as the identification and transition phases proceed.

The costs associated with this PQC migration may be reduced by utilizing existing IT equipment lifecycles and system modernization plans. To do so, it is critical to perform the initial phases of this plan quickly to identify where these cost efficiencies can be leveraged. Delays resulting in rushed procurement will increase costs.

3.1.3 Education strategy

It is important that staff across the organization are aware of the quantum threat and the impact it may have on the systems they use or are responsible for. The TBS GCxchange platform will be leveraged to share artifacts with departments and agencies, including material produced by the Cyber Centre, such as presentations and publications for a variety of audiences. The Cyber Centre's Learning Hub will provide course material to educate on the quantum threat to cryptography. Senior executives must be briefed to be aware of the impact the migration to PQC will have on their operations.

As the PQC migration progresses, it's important to keep senior executives informed of developments and progress, including any emerging challenges or roadblocks that teams may face.

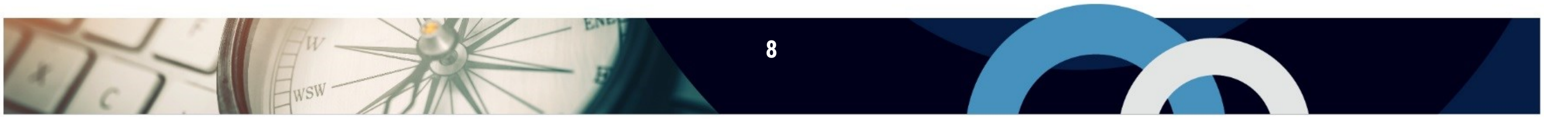
3.1.4 Procurement policies

To maximize the lifetime of new systems, departments and agencies should ensure new procurements have requirements that support PQC. The Cyber Centre strongly recommends that systems employ established cyber security standards. Following standards provides assurance of independent security review and promotes interoperability to avoid vendor lock-in. Some cyber security standards are still being revised to support PQC. The Cyber Centre is updating Guidance for securely configuring network protocols (ITSP.40.062) as PQC support is finalized in standards. It is expected that support for PQC may not be currently available in some product categories.

The Cyber Centre has recommended contract clauses for systems containing cryptographic modules. These are available upon request and will be made more widely available. In general, departments and agencies should consider the following best practices for procurements:

- contracts have clauses to ensure that the vendor will include support for PQC that is compliant with Cyber Centre recommendations in Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111)
- cryptographic modules have been certified by the Cryptographic Module Validation Program
- support for cryptographic agility to allow for future configuration changes

The earlier PQC is included in procurement clauses, the lower the costs departments will face during the migration.



3.1.5 Plan approaches for identification

The next phase in this roadmap is the identification of where cryptography is used in IT systems. Sometimes called cryptographic discovery, this identification is necessary to create an inventory of systems that need to be transitioned. The departmental PQC migration plan must include the approaches that will be undertaken to identify systems and build this inventory. More detail on identification is provided in the next section.

3.2 Identification

Identifying where and how cryptography is used is a critical step in the process to migrate to PQC. Systems using cryptography will include:

- network services
- operating systems
- applications
- code development pipelines
- all physical IT assets, such as
  - server racks
  - desktops
  - laptops
  - mobile telephones
  - network appliances
  - printers
  - voice over Internet Protocol telephony
  - hardware security modules
  - smart cards
  - hardware tokens

These may be hosted on-premises, within contracted IT platforms, or a cloud service provider, or under employee possession. The scope is wide, thus making identification a challenging task.

The information gathered in this phase will be used to create an inventory that should include the following information per system:

- system components employing cryptography
- vendor and product version for each of the components
- security controls that rely upon the identified cryptography[4]

[4] IT security risk management (ITSG-33): Annex 3A - Security control catalogue: https://www.cyber.gc.ca/en/guidance/annex-3a-security-control-catalogue-itsg-33

- applicable network security zones
- current cryptographic configurations
- hosting platform
- system dependencies
- relevant service contracts and expiry dates
- expected refresh year for the system or its components
- responsible departmental point of contact
- if the system should be prioritized for migration

Other technical information may be relevant to include in the inventory. The Cyber Centre will provide additional guidance to departments as experience grows within the GC.

Departments must identify systems that are a high priority for migrating to PQC. Systems protecting the confidentiality of information in transit over public network zones[5] may be at risk earlier than expected due to the harvest now, decrypt later (HNDL) threat. A HNDL threat is when a threat actor intercepts encrypted information, stores it and then decrypts it in the future, when sufficiently powerful quantum computers exist. It is recommended that any systems susceptible to a HNDL threat be a high priority for migrating to PQC. Other considerations include the information lifespan, support for cryptographic agility, and the impact of compromise. It may be valuable to complete a risk assessment for the quantum threat to ensure that systems are properly prioritized.

Discovery of systems containing vulnerable cryptography should utilize multiple methodologies. Leveraging existing IT service management (ITSM) processes within the organization may be an efficient way to produce an initial departmental inventory. Lifecycle and change management committees should have much of the information needed for an inventory system entry. However, in practice, ITSM maturity may vary across departments.

Software tools and services will be necessary to complete cryptographic discovery. This may leverage existing cyber security services, such as security information and event management (SIEM) solutions, network monitoring and inspection, and endpoint detection and response (EDR) technologies. These services may require configuration changes, third-party plugins, or additional filters to identify the use of cryptography. Independent tools for cryptography discovery will employ technology for scanning networks, hosts, log files, or source code. The Cyber Centre's sensors program is a tool expected to assist departments in identification. Additional guidance on cryptographic discovery tools and services will be provided to departments by the IT Security Tripartite, which includes TBS, SSC, and the Cyber Centre.

It is important to not be overwhelmed in completing the discovery and to begin with an initial, incomplete inventory with actions to iteratively improve the data.

During the identification phase, departments should use the inventory to engage relevant IT vendors and contractors to determine their plans to implement PQC in their products and services. Understanding which system components will be eligible for upgrades versus replacement will assist in the next phase of developing a transition plan.

[5] Baseline security requirements for network security zones (ITSP.80.022): https://www.cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-version-20-itsp80022

3.3 Transition

The transition phase leverages the inventory created in the identification phase to plan and execute system upgrades, replacement, tunnelling, and/or isolation.

In addition to the inventory data, the plan must consider departmental resources for identifying and assessing solutions, performing necessary procurements, testing, and deployment. The plan for each system will typically require multiple stages and should be integrated with existing IT change management processes to ensure proper preparation including:

- an impact assessment
- a rollback playbook
- a staging environment for testing changes
- monitoring to validate successful operation post-transition

For each system, technical teams must identify and assess solutions to incorporate PQC or otherwise mitigate the quantum threat. The availability of PQC-capable products may be limited in the early stages, but vendors are rapidly adopting PQC as updates to protocol standards are completed. Solutions should meet all the procurement requirements established in the Preparation phase (Procurement policies 3.1.4).

Many systems will need to maintain backwards compatibility to allow for continued operation with non-transitioned systems for a period of time. The first stage for a system transition may be to support the use of PQC, followed by a second stage to disable the vulnerable, legacy cryptography.

It may not be feasible to transition some legacy systems to use PQC without a full system replacement. To meet migration milestones, it may be necessary to isolate such systems on the network or to tunnel traffic within a PQC-protected encapsulation layer. Such decisions should be made during the transition phase planning.

Early versions of the departmental PQC migration plan may offer limited detail on the transition phase; however, this section should be expanded as identification efforts progress.

4 Milestones and deliverables

Milestones and deliverables for federal departments and agencies are as follows:

- April 2026: Develop an initial departmental PQC migration plan
- Beginning April 2026 and annually after: Report on PQC migration progress
- End of 2031: Completion of PQC migration of high priority systems
- End of 2035: Completion of PQC migration of remaining systems

These milestones for the completion of migrations implies that quantum-vulnerable algorithms are disabled, isolated or tunnelled. That is, rather than just supporting PQC, the quantum risk has been mitigated. It will be critical for departments and agencies to create, revise and follow their departmental PQC migration plan to migrate systems as early as possible to meet the milestone dates.

More information on expectations for reporting progress is given in the next section.

5 Governance and coordination

5.1 Relevant Government of Canada governance bodies

Departments and agencies are accountable for managing cyber security risks in their program areas. However, GC-wide initiatives, such as this migration to PQC, requires a whole-of-government approach managed at the enterprise level in accordance with accountabilities outlined under the TBS policy instruments.

The IT Security Tripartite consists of the TBS, SSC, and the Cyber Centre. The tripartite is a centralized body that provides advice, guidance, oversight, and direction on GC-wide cyber security initiatives such as the GC migration to PQC. The tripartite supports departments and agencies under TBS authorities.

The GC Enterprise Architecture Review Board (GC EARB) provides a governance mechanism to assess if proposed enterprise systems are aligned to the GC Enterprise Architecture Framework. The framework ensures business, information, application, technology, security, and privacy architecture domains meet the Service and Digital Target Enterprise Architecture. Cyber security requirements, such as compliance to the Cyber Centre's cryptographic recommendations, are part of the GC Target Enterprise Architecture which is aligned with overall TBS strategic direction and TBS policy instruments.

The GC has interdepartmental Quantum Science and Technology (S&T) Coordination Committees at senior executive levels to synchronise efforts and maintain Canada's leadership in quantum S&T. These committees oversee the federal government's actions supporting Canada's National Quantum Strategy (NQS), including the NQS roadmap on quantum communication and post-quantum cryptography.

5.2 Reporting on progress

Monitoring the progress of the GC migration to PQC is essential for effective activity oversight and governance. This ensures accountability and the completion of milestones. TBS oversees compliance to its policy instruments in accordance with the Treasury Board Framework for Management of Compliance. It also tracks progress on the departmental plan on service and digital which includes cyber security, as required under the Policy on Service and Digital. Reporting on departmental progress and on the activities needed to complete the migration to PQC will be requested and collected by TBS as part of the annual submissions for the departmental plan on service and digital.

5.3 Additional resources and support

The TBS GCxchange platform will be leveraged to share artifacts with federal departments and agencies to assist in the migration to PQC. The Cyber Centre will continue to publish guidance and recommendations for organizations on the Cyber Centre website.

Please use the Cyber Centre contact information at the top of this page to request more information on the quantum threat, PQC, or this roadmap.