



PSCIOC Debrief

FEBRUARY 22, 2023



FPT SYMPOSIUM
on Digital Trust & Cybersecurity



BRITISH
COLUMBIA

COLOMBIE-
BRITANNIQUE

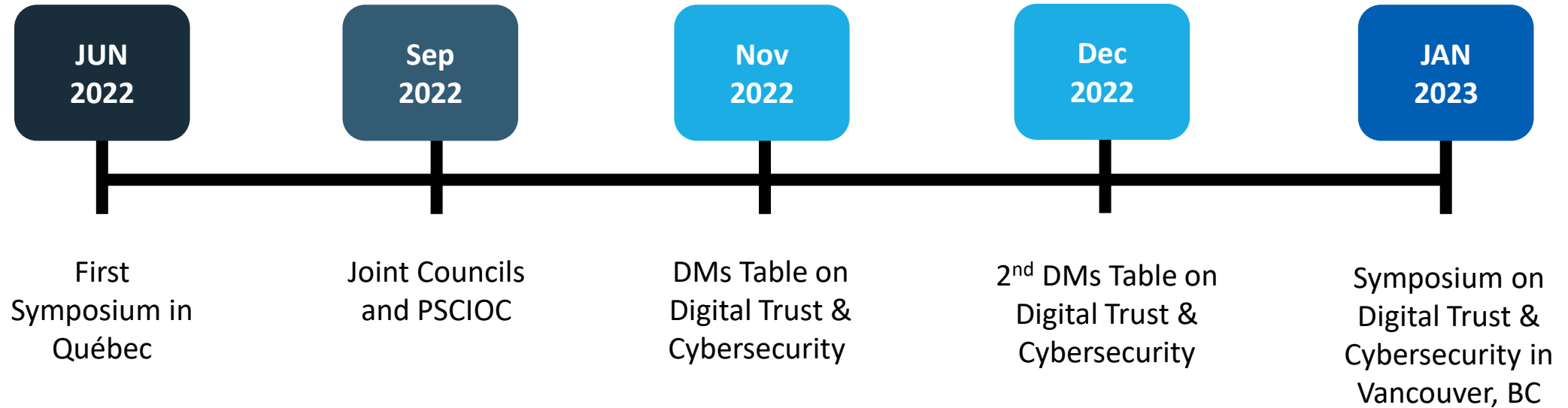
Agenda

- A. Symposium Debrief
- B. Proposed Approach
- C. Facilitated Discussion
- D. Timing and Logistics
- E. Next Steps

A. Symposium Debrief

A. SYMPOSIUM DEBRIEF

Recap & Timeline



Québec Recap – June 2022

FOCUS AREAS

1

Digital identity
a shared platform for all
jurisdictions to develop
interoperable services

2

National Agreements
on information and
expertise sharing

3

**Standardization &
harmonization of the
technologies**

SHARED PRIORITIES

1. Increasing **use of
digital channels**
among Canadians

2. Protecting against
increasing **cyber
attacks**

3. Managing **costs**

4. Finding **skilled
resources**

BC Recap – January 2023

- The symposium signalled a commitment from governments to take the lead in protecting personal information in the digital world, and a commitment to working collaboratively across Canada.
- 12 Ministers from across Canada, 2 virtually, over 60 attendees.
- 1 ½ days in Vancouver British Columbia, January 24th & 25th.

Jurisdictional showcases

Québec, Alberta,
Nova Scotia, Ontario,
BC

Panel 1

Strength in Numbers:
Pan-Canadian
Collaboration on
Cybersecurity

Panel 2

Enabling Indigenous
languages in identity
records/systems

Roundtable

Deputy and Minister
concurrent in camera
roundtables

Actions and Decisions

ACTION

Ministers and DMs Tables endorsed the development of a **Pan-Canadian Workplan** focused on the priorities related to digital trust, credentials, cybersecurity and work on enabling Indigenous languages in identity systems.

DECISION

Ministers in support of an **annual meeting**. Ontario offered to host the September 2023 meeting in Niagara. Newfoundland and Labrador offered to host the meeting in June 2024.

Focus Areas

Building off the focus areas identified in Québec, Ministers identified the following*:

1

Cybersecurity
jurisdictional
information sharing
and finding, and
developing skilled
resources

2

**Digital trust and
credentials**
a focus on
interoperability,
collaboration, and
coordinated
communications

3

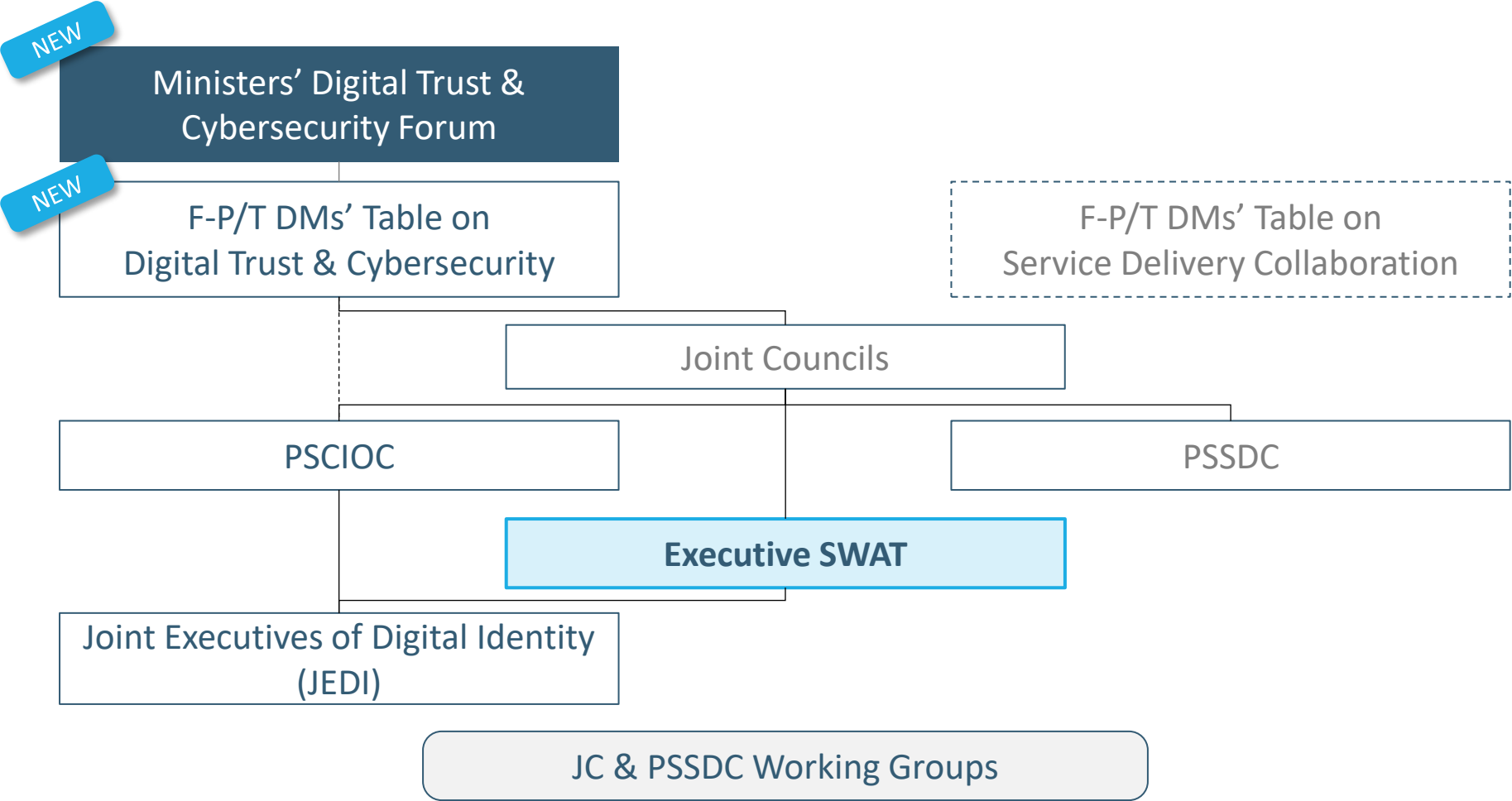
**Indigenous languages
in identity systems**
with Indigenous
communities,
mapping the barriers,
tools and
opportunities

*RoD Action Details in [Appendix](#)

B. Proposed Approach

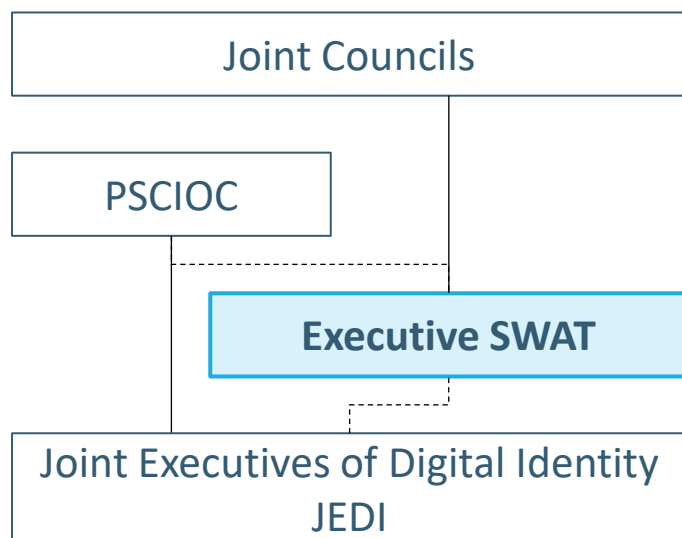
B. PROPOSED APPROACH

Current Structure



B. PROPOSED APPROACH

SWAT Role



The decision to create the SWAT team was made by the Joint Councils on June 28, 2022.

Tasked to identify key roles, supports and leadership needed to provide backbone support to enable the success of the Pan-Canadian Digital Trust & Credentials Program.

AND develop, support and implement Pan-Canadian efforts towards Digital Trust, Credentials and Cybersecurity priorities.

B. PROPOSED APPROACH

Executive SWAT Membership

JURISDICTION	NAME	TITLE	EMAIL ADDRESS
Institute for Citizen-Centred Service (Co-Chair)	Peter Watkins	Pan-Canadian Digital ID Program Executive	Peter.Watkins@iccs-isac.org
Nova Scotia (Co-Chair)	Natasha Clarke	Associate Deputy Minister & Chief Digital Officer	Natasha.Clarke@novascotia.ca
Government of Canada (TBS)	Paul Wagner	Deputy Chief Information Officer, Treasury Board of Canada Secretariat	Paul.Wagner@tbs-sct-gc.ca
British Columbia	CJ Ritchie	Associate Deputy Minister and Government Chief Information Officer	CJ.Ritchie@gov.bc.ca
Ontario	Rob Devries	Assistant Deputy Minister, Platforms, Ontario Digital Service	Robert.Devries@ontario.ca
Québec	Jonathan Kelly	Secrétaire adjoint du Centre québécois d'excellence numérique, Ministère de la cybersécurité et du numérique	Jonathan.Kelly@mcn.gouv.qc.ca
Prince Edward Island	Tracy Wood	Chief Digital and Operating Officer	TMWOOD@gov.pe.ca
Yukon	Mark Burns	Director, eServices, Information & Communications Technology	Mark.Burns@yukon.ca
Alberta	Gene Smith	Chief Digital Officer	Gene.Smith@gov.ab.ca
Municipal Information Systems Association (MISA)	Harry Turnbull	MISA Ontario, Director of Municipal Modernization and Partnerships	harry@misa.on.ca
Institute for Citizen-Centred Service	Dan Batista	Executive Director	Dan.Batista@iccs-isac.org

B. PROPOSED APPROACH

SWAT Approach



B. PROPOSED APPROACH

Current Working Groups

JOINT COUNCILS

• Mechanism for FPTM jurisdictions to collaborate and learn from each other on the use of Open Source software and approach of working in the open.

Open Source Working Group



• Accelerating work to deliver trusted digital identity for Canadians. Digital identity is a key foundational element in transforming services.

Digital Trust & Credentials Program



• National forum for the exchange of information relating to ATI/FOI and privacy research, best practices, training, IT products, and other resources.

Privacy Sub-Committee



• Responsible for the conduct of research to support the public sector inter-jurisdictional CIO and service delivery communities.

Research Committee



• Share information, experiences and explore inter-jurisdictional opportunities to collaborate on tangible service improvements for Canadian

Service to Business Working Group



• Improving the client experience by leveraging government and Open Data and advanced analytics to improve service.

Data Driven Intelligence Working Group



• Responsible for the annual refresh and promotion of the Analytics Playbook.

Analytics Playbook Sub-Group



DIRECT INVOLVEMENT

SUPPORTED BY

PSCIOC

• National forum to understand the experiences of other jurisdictions that have adopted Microsoft Office 365 in their IT environment.

Microsoft Office 365 Working Group



• National forum to exchange information, policies, security awareness program practices and architecture initiatives related to information protection and cyber security.

National CISO Committee on Information Protection



Endorsement Request

- Reaffirm mandate and delegation of **Executive SWAT** team
- Confirm that SWAT Team will:
 - Vet and develop ICCS **Digital Trust and Credentials** team
 - Work with ICCS and PSCIOC to develop **Pan-Canadian Workplan** including specific inter-jurisdictional pilot initiatives that align with Ministers' priorities.
 - Develop forward agenda for PSCIOC, Joint Councils, and DMs based on the workplan

C. Facilitated Discussion

Roundtable

Guiding questions (~5 minutes each):

- 1) What work is underway in your jurisdiction that supports pan-Canadian efforts? Are there misalignments or additional priorities with the work in your jurisdiction that should be considered for the workplan?
- 2) What pilots or deliverables do you foresee being included in the workplan?
- 3) With respect to working groups, are there functions missing or groups you feel may need to shift their existing workplans to better support the new Pan-Canadian workplan? Please share any additional or refocused items that should be included these groups.

D. Timing and Logistics

Terms of Reference

CURRENT

Statement of Objectives

1. Provide a forum for open communication between members to exchange information, best practices and ideas and to provide support and advice to CIO peers on matters relating to:
 - the effective management and use of information and technology in support of public sector programs and objectives;
 - IT products and services including the involvement of the private sector in the management and service delivery of public sector IM and/or IT.
2. Provide leadership by initiating and supporting IM and/or IT-related
 - communities of practice and
 - collaborative projects to garner mutual benefit and economies of scale for municipal, provincial, territorial or federal governments.

PROPOSED ADDITION

3. Develop and deliver on Ministers' priorities for Digital Trust and Cybersecurity.

D. TIMING AND LOGISTICS

Current

No formal Deputy or Minister involvement.

DAY 1

Learning Event (host)

Joint Councils Members and
Observers

DAY 2

PSCIOC and PSSDC

Concurrent meetings
Members and Observers

DAY 3

Joint Councils

Joint Councils Members and
Observers

D. TIMING AND LOGISTICS

Proposed

Embed Ministers and Deputies into three day in person events

DAY 1

Ministers Symposium

Ministers and Deputy Ministers
or Equivalent

Learning Event (host)

Joint Councils Members and
Observers

DAY 2

Deputy Ministers Table

Deputy Ministers or Equivalent

PSCIOC and PSSDC

Concurrent meetings
Members and Observers

DAY 3

Joint Councils

Joint Councils Members and
Observers

Appendices

Reference Materials

- 01. Symposium Summary Note**
- 02. Record of Decision Vancouver Symposium**
- 03. Joint Councils Working Groups and Communities of Practice (Materials from JC TAB 4)**
- 04. PSCIOC Terms of Reference**

RoD Action Details

Action Item #1

Recommendations:

- Improving cybersecurity posture across jurisdictions by a shared approach to information sharing, as a critical service (sharing info on best/next practices, lessons learned, ransomware). A consistent and comprehensive living set of agreements to protect Canadians and respond to any threats across all levels.
- Looking at different approaches to address the critical digital and cyber talent gap - recruitment, training / redeployment, and retention. Building the next generation of digital/cyber talent.

Action Item #2

Recommendations:

- Mapping the barriers to Indigenous names to identity immediate next steps
- Mapping of digital tools that have been developed and are available for opportunity to leverage
- Collaboration and consultation approach with Indigenous voices in this work

Action Item #3

Ministers and DMs Tables endorsed the development of a Pan-Canadian Workplan focused on the priorities related to digital trust, credentials and cybersecurity and work on enabling Indigenous languages in identity records.

RoD Action Details

THEME	MINISTERS	DEPUTIES
Develop a Pan-Canadian Workplan	Consensus to develop a pan-Canadian workplan for the Ministers' Table	Agreed, and consensus for DMs to develop the workplan with support from Joint Councils, and the Public Sector CIO Council (PSCIOC).
	Encourage jurisdictions to use open code so we can all benefit	Agreed
Collaborate on Digital Trust	Continue inter-jurisdictional collaboration on Digital Trust and Cybersecurity	Agreed
	Work to ensure pan-Canadian digital trust and credentials interoperability	Agreed
	Recognition of cross jurisdictional work on projects already underway	Build on and share cross jurisdictional work on projects already underway
		Partner on communications and consultation of Canadians.
Collective Action on Cybersecurity	Improving cybersecurity posture, training, and ransomware response	Agreed
	Jurisdictional Information sharing	Agreed, leverage existing structures, such as NCCIP, to accelerate. Create a consistent and comprehensive living set of agreements to protect Canadians and respond to any threats across all levels.
		Develop a shared set of cybersecurity incident response experts
Build and Retain Digital & Cybersecurity Talent	Work on digital staffing and retention	Agreed, looking at different approaches including recruitment, training, redeployment, and retention. Building the next generation of digital/cyber talent.
Enable Indigenous languages in identity records/ systems*	In collaboration with Indigenous communities, mapping the current barriers, legislative, policy, and practice, and the existing tools in use.	

Statement of Intent

MINISTERS' SYMPOSIUM ON DIGITAL TRUST AND CYBERSECURITY

Canadians and Canadian businesses are increasingly choosing the convenience and immediacy provided by digital services. However, data and security breaches, fraud, and other abuses that complicate service delivery are also on the rise.

We share the common goal of empowering people and businesses to participate confidently and securely in the digital world. Each government will provide trustworthy and privacy-protecting digital credentials that will improve digital services across the economy, with regards to our respective responsibilities in terms of cybersecurity and digital trust. Our work will be guided by the digital principles and service standards of our jurisdictions.

Énoncé d'intention

MINISTERS' SYMPOSIUM ON DIGITAL TRUST AND CYBERSECURITY

Les Canadiens et les entreprises canadiennes sont de plus en plus nombreux à choisir des services numériques pour leur côté pratique et leur immédiateté. Toutefois, les vols de données et violations de sécurité, les actes de fraude et autres actes illicites qui compliquent la prestation des services sont également de plus en plus fréquents.

Nous avons une priorité commune de donner aux individus et aux entreprises les moyens pour qu'ils participent en toute confiance et de manière sécuritaire dans le monde numérique. Chaque gouvernement souhaite fournir des identités numériques de confiance et des attestations qui protégeront la vie privée en plus d'améliorer les services numériques dans toutes les sphères de l'économie, dans le respect de nos responsabilités respectives en matière de cybersécurité et de confiance numérique. Notre travail reposera sur des principes en matière de numérique et sur des normes de services propres à chaque province et territoire.