



Government
of Canada

Gouvernement
du Canada

CANADA'S DIGITAL INTERCHANGE (CDI)

Moving beyond the business case
to enabling digital service

Joint Councils
September 14, 2016

PRESENTATION OBJECTIVES

- 1 Provide background on service delivery and digital identity imperative
- 2 Provide conclusions from the CDI Business Case
- 3 Communicate next steps

THE SERVICE LANDSCAPE IS SHIFTING

- Innovations in private sector service delivery – driven by advancements in technology and the rise of a dynamic mobile experience – are increasing citizens' and businesses' expectations.
- Change is needed to meet client expectations for fully online services.
- The recently-issued ministerial mandate letters clearly outline the government's service improvement priorities including:
 - developing new services and strategies;
 - improving and expanding existing services; and,
 - implementing new service standards and performance measurement and reporting.
- In the mandate letter to the President of the Treasury Board, the Prime Minister requested that the President develop, in collaboration with the Minister of Families, Children and Social Development, a new **service strategy** that aims to create a single online window for all government services with new **performance standards** as well as rigorous assessments of the performance of key government services.



DIGITAL IDENTITY SERVICES

Part of government response to improving GC service delivery and security

- Identity is fundamental to Canadian society as it is the starting point of trust and confidence in interactions between the public and governments and government to government.
- **Canada's Digital Interchange (CDI)** underpins the service strategy as it is the vehicle that will allow for confirming identity information, retrieval of identity information and notification of change in identity information.
- It will enable secure online service delivery and service bundles, program integrity, stronger service partnerships with other levels of government and towards an integrated “tell us once” service experience.
- CDI is a pan-Canadian initiative that will provide real-time, cost-effective digital identity services that will allow federal, provincial, territorial and municipal governments to securely confirm an individual's identity leading to increased convenience and reduce processing time and administrative burden on clients.

All jurisdictions and sectors have a role to play

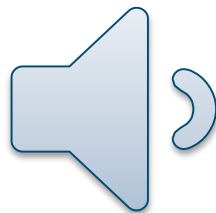
- ✓ PTs are the authoritative sources of identity information for persons born in Canada in their respective jurisdictions.
- ✓ The federal government is the authoritative source of identity information for persons born abroad

CDI – A KEY ENABLER FOR DIGITAL SERVICE



VALIDATION

VALIDATION is the confirmation of personal identity information (e.g., birth, death, immigration status) across all levels of government. Validations are true or false responses, and are based on a pan-Canadian standard (e.g.: *This person is applying for a driver's licence. Please confirm the name, date of birth and citizenship of this individual is correct*).



NOTIFICATION

The **NOTIFICATION** of a change in personal identity information based on life events (e.g.: *This person has died; please update your databases*). This may trigger a review of continued eligibility/entitlement.



RETRIEVAL

The **RETRIEVAL** of personal identity information, which is a validation plus a request for some additional related information. Departments must show that they have the authority to collect this additional information (e.g.: *This person is applying for a driver's licence. Please confirm the name, date of birth and citizenship of this individual is correct, and tell me any additional aliases that you have on file*).

CDI is neither a replacement for in-person service channel nor a national ID Card or national ID database.

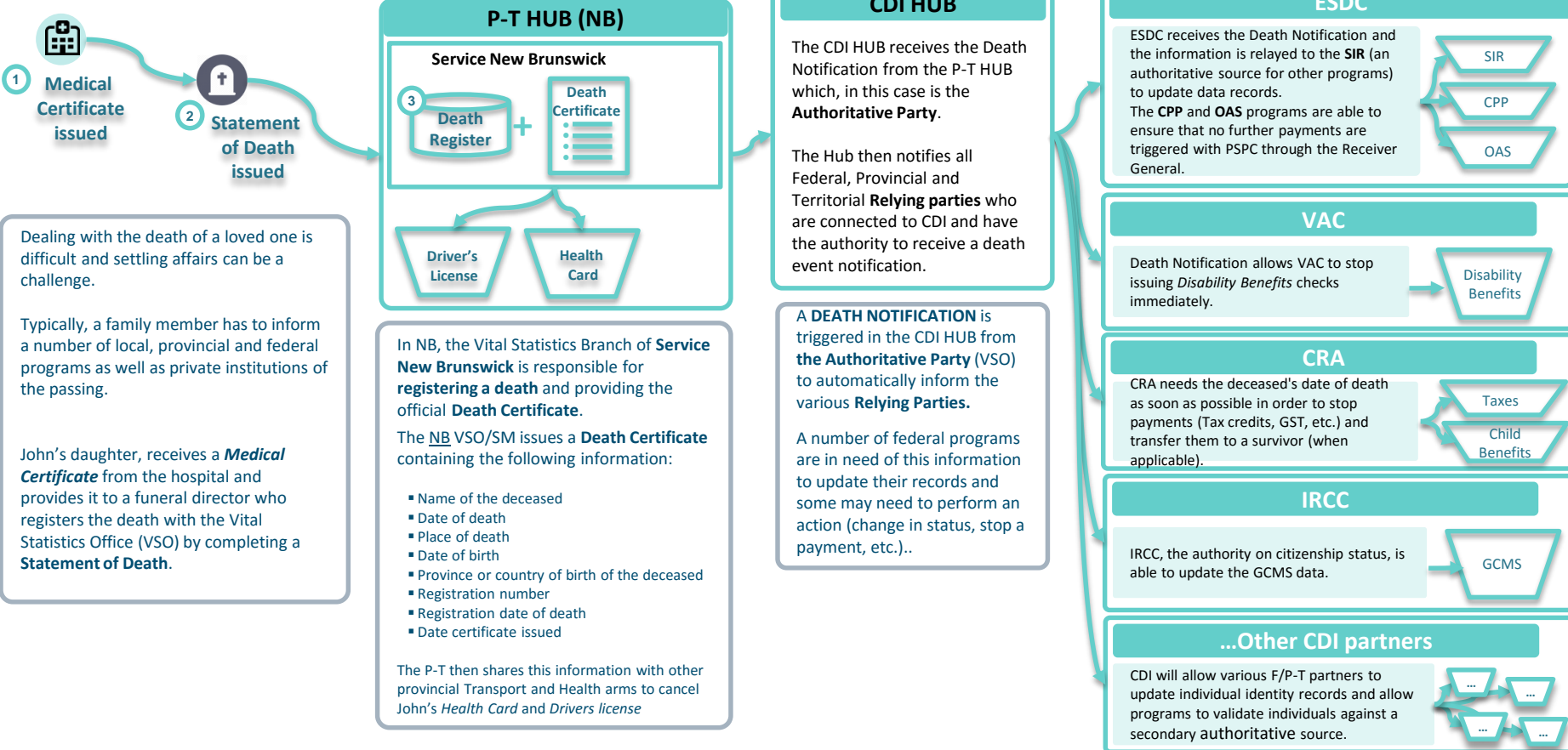
A real-time, scalable, cost-effective service that will enable all levels of government to securely confirm an individual's identity information, to support online services to clients across Canada.

Tell Us Once - How it works

DEATH NOTIFICATION



John just died at the age of 74. He was a retired veteran who lived in Moncton, NB. At the time of his death, he was receiving CPP, OAS as well as additional support from Veterans Affairs Canada for his military service (disability benefits).



Many steps are required to enable **"Tell us Once"** initiatives.

- A mature CDI will allow departments to simplify the interactions they do with citizens at large (e.g.: not ask for information multiple times if an authoritative party has already validated it).

WORK ACCOMPLISHED - February to September 2016

Since last update to Joint Councils in February, number of key milestones completed:

- ✓ Finalized analysis of federal business needs and legal authorities
- ✓ Finalized preliminary analysis of provincial/territorial business needs
- ✓ Finalized options for governance models
- ✓ CDI business case completed
- ✓ Met with Office of the *Privacy Commissioner*

Canada's Digital Interchange – PT Engagement

ONGOING

- PT engagement through the Project Oversight and Coordination Committee (POCC) meet regularly via teleconference

DECEMBER 2015

- CDI status report was presented, presented plan to provide draft business case in **Spring 2016**

JANUARY 2016

- CDI business needs questionnaire was sent to POCC members to inform the CDI Business Case.
- **BC, ON, QC, and NB responded to the business needs questionnaire.**

MAY 2016

- Progress on CDI presented to FPT DM Table on Service Delivery Collaboration
 - Update on Pan-Canadian Trust Framework
 - CDI Business Case update
 - Federal and PT business needs
 - Authorities and information sharing agreements
 - Examining possible governance approaches

CDI BUSINESS CASE COMMENTS – From PTs

JULY 2016

PTs were asked to provide comments on the CDI Business Case

- ✓ **Municipalities need recognition** - General consensus is that municipalities are underrepresented in the business case. Further analysis on how municipalities will play a part in CDI will occur in the future.
- ✓ **Business needs are very federal focussed** - PT business needs were requested in December 2015 but only a few partners chose to participate, making it difficult to provide the same level of detail for PT business needs.
- ✓ **Technical costs are included, but non-technical costs need to be identified** - Changes to processes, policies, procedures or legislation will be explored in the future.
- ✓ **Retrieval function not required** - AB indicated that they do not support having a retrieval function. Further, legislation related to accessing citizen data maintained by Motor Vehicles, Health will not allow this function to proceed.
- ✓ **Central hub architecture may not be needed** – AB indicated that they do not see the value of the central hub architecture if they simply wish to connect to other provinces. The central hub is a possible architecture that is explored in the business case but further analysis is required.
- ✓ **Changes to legislation/privacy acts may take longer than anticipated** – Proper analysis of how long it will take to change barriers to information sharing needs to take place in order to properly determine when CDI can launch.

Canada's Digital Interchange – PT Engagement

AUGUST 2016

- PT feedback incorporated into business case

SEPTEMBER 2016

- Joint Councils meeting – presentation of CDI Business Case and request for input on governance

NEXT STEPS

Phase I (Now – March 2017)

- Develop federal infrastructure/hub to support information sharing between federal departments and agencies
- Resources given to support the improvement of Death Registration and Notification processes
- Undertake a Request for Information process to identify potential options for a full Pan-Canadian build in Phase II
- Engage with PTs to finalize:
 - a governance structure
 - costing and transaction fee models
 - design elements required by partners (standards, technology, etc.)

Phase II (April 2017 – March 2020)

- Implementation of governance structure
- Creation of Pan-Canadian CDI Hub
- Onboarding of all partners

CDI BUSINESS CASE - Conclusions

Business case provides a strong rationale for CDI and recommendations for moving forward

- ✓ **Validation, Notification and Retrieval of identity information** were key business needs identified by both federal and P/T partners .
- ✓ **Federated and interoperable solution** that is **scalable**, primarily **focused on the verification of identity information** that can expand to **include other partners and attributes over time** was identified as the scope for CDI.
- ✓ **Value proposition for CDI has three pillars:**
 - improved service experience for individuals;
 - improved service experience for business by bringing more programs and services online and integrate towards a “tell us once” approach ; and,
 - promoting confidence to clients that privacy safeguards are in place to ensure personal information is handled fairly and transparently.
- ✓ **Benefits realization categorized into three distinct categories :**
 - direct cost avoidance (reduction of in-person channel, administrative overhead for ISA);
 - indirect cost avoidance (improving program integrity, reducing overpayments); and,
 - overall service improvements (service bundling, one-stop, predictive services)
- ✓ **Broad changes to enabling legislation preferred** over targeted approach.

CDI BUSINESS CASE - Conclusions (con't)

- ✓ **Changes to enabling legislation** to be lead through **Service Strategy** development.
- ✓ **Multilateral framework for privacy considerations and information sharing agreement (ISA)** identified.
- ✓ **Multi-tiered** (priority setting, operational oversight and management, service provider) **pan-Canadian governance structure with strategic oversight representation from all member jurisdictions** (e.g., FPT DM Table on Service) approach to governance identified.
- ✓ **Preliminary technical cost** estimates, for the scaled three component infrastructure build, are based on RFI responses and other comparables within federal government
 - federal infrastructure build \$6M-\$12.4M + incremental costs based on number and type of services
 - pan-Canadian infrastructure build \$19.7M-\$39.4M + incremental costs
 - PT infrastructure build + incremental costs based on number and type of services
- ✓ **Funding formula** will be subject to negotiations with PTs

CDI BUSINESS CASE COMMENTS – From PTs

PTs were asked to provide comments on the CDI Business Case

- ✓ **Municipalities need recognition** - General consensus is that municipalities are underrepresented in the business case. Further analysis on how municipalities will play a part in CDI will occur in the future.
- ✓ **Business needs are very federal focussed** - PT business needs were requested in December 2015 but only a few partners chose to participate, making it difficult to provide the same level of detail for PT business needs.
- ✓ **Technical costs are included, but non-technical costs need to be identified** - Changes to processes, policies, procedures or legislation will be explored in the future.
- ✓ **Retrieval function not required** - AB indicated that they do not support having a retrieval function. Further, legislation related to accessing citizen data maintained by Motor Vehicles, Health will not allow this function to proceed.
- ✓ **Central hub architecture may not be needed** – AB indicated that they do not see the value of the central hub architecture if they simply wish to connect to other provinces. The central hub is a possible architecture that is explored in the business case but further analysis is required.
- ✓ **Changes to legislation/privacy acts may take longer than anticipated** – Proper analysis of how long it will take to change barriers to information sharing needs to take place in order to properly determine when CDI can launch.

Note: AB, ON, QC, and YK provided comments.

WAY FORWARD

» To maintain momentum, three parallel tracks of work are being undertaken:

Analysis of key issues of federal interest

Analysis on **key issues of federal interest** that will enhance information for decision making

- Implementation / sequencing
- Identify early wins
- Costing
- Interoperability

Engagement with PT partners

Continued **engagement with PT partners**

- Governance (engage FPT joint councils)
- Costing
- Technical options

Seeking a mandate

Seek policy authority for CDI

ANNEXES

CDI BUSINESS CASE: Key Conclusions

Scope

- Designed as a scalable solution, CDI will be an interoperability solution primarily focused on the verification of identity information that can be expanded to include other partners and other attributes over time.
- Benefits realised will include direct cost savings, indirect savings and service improvements for all partners.

Business Needs

- Validation, Notification and Retrieval of information were identified as the key functionalities needed from both federal and P/T partners.
- From federal partners, majority of needs focused on need to confirm identity information.
- Various states of readiness, P/T→P/T connections, revenue generation top of mind, IRCC data valuable.

Authorities and Privacy

- Majority of departments have authorities to exchange information, issue remains with enabling legislation and ISA requirements.
- Making changes to enabling legislation preferred to targeted approach, enables long-term vision for additional CDI partners and multilateral frameworks for privacy considerations and ISAs.

Governance

- To be a truly pan-Canadian service, the governance needs strategic oversight representative of all member jurisdictions (e.g., FPT DM Table on Service).
- Operational oversight and management will also be representative of all partners (e.g., shared governance corporation or multilateral framework agreement).
- Service provider to build and/or administer the CDI service include public and private options.

Costing

- Key costing components of a CDI service have been identified with elements costed at “high/low” range including use of “TBD” for unknown costs for business case, using estimates generated from internal sources, will continue to seek additional clarification for anticipated PT costs.

COST BENEFIT – Details

Cost

- Preliminary costing estimates* are based on a centralized, pan-Canadian hub
 - Federal infrastructure build cost (low end of \$6M to high end of \$12.4M)
 - Federal service development cost - \$500K for each service per department (notification, validation or retrieval)
 - Pan-Canadian infrastructure build, partner connections and onboarding costs (low end of \$25.7M to high end of \$58.1M)
- Based on estimates from RFI done in 2015, private sector estimates for the build component are similar to public sector estimates
- A more detailed RFI will be required to obtain updated private sector costs that reflect the preferred architecture

* costing estimates based on a series of assumptions that are outlined in the business case, and are comprised of estimates for those elements that were able to be identified. There are additional unknown costs that will need to be factored based on further discussions with partners.

Benefits

- Increased confidence of identity assurance allows for greater on-line service offerings
- Enables a multi-channel service delivery approach
- Provides clients with an option to reuse information already given to a partner government agency to meet identity assurance needs
- It is difficult to ascertain how much overpayments and fraud are specifically due to lack of rigorous identity information, however estimates below illustrate the scope of the problem:
 - **\$20.6M** in overpayments reported by veterans Affairs Canada in FY 2012-13
 - **\$600M** in overpayments reported (partially identity related) by the Auditor General of Ontario in 2009 for Ontario Works
 - **\$260M** in health care fraud in BC (due to fraudulent CareCards) in 2011

PRIVACY - Embedded into design

Incorporating the seven *Privacy by Design** principles within CDI

- 1 **Be preventative, not remedial.** Anticipate and prevent invasive events before they happen, not scramble to manage after a breach.
- 2 **Lead with privacy as the default setting.** Ensure personal data is automatically protected; don't require users to take extra steps to do so.
- 3 **Embed privacy into the design.** Privacy measures should be fully integrated components, not added on later.
- 4 **Retain full functionality.** Privacy and security are equally important; neither should be compromised for the other.
- 5 **Ensure end-to-end security.** All data should be securely held while it's needed and destroyed when it's not.
- 6 **Maintain visibility and transparency.** Assure stakeholders that business practices and technologies involved are transparent to the end-user and subject to independent verification. Remember: it's not your data.
- 7 **Respect user privacy.** Individual interests must be supported by strong privacy defaults, appropriate notice and user-friendly options.

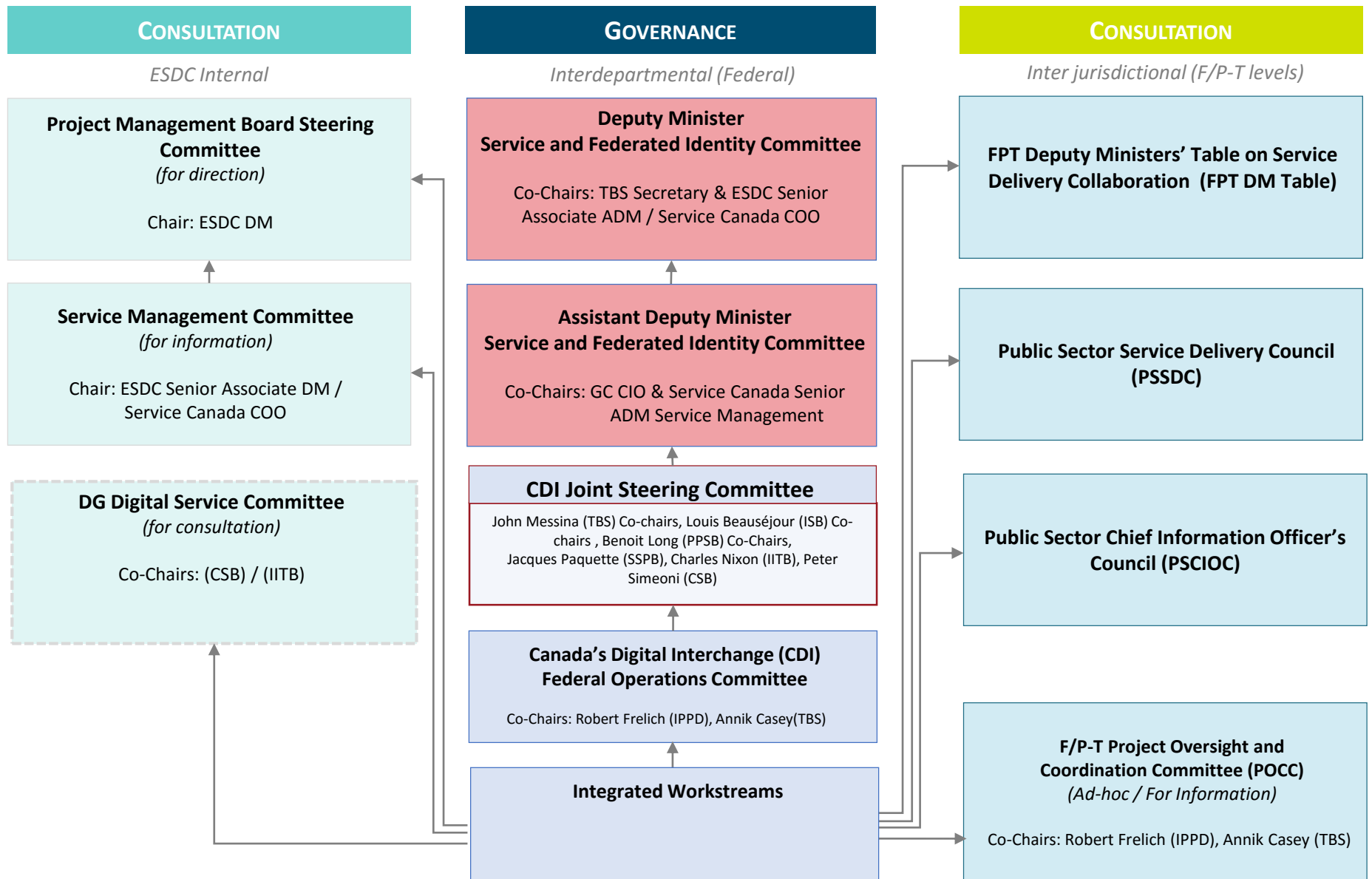
Privacy by Design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices..

* Dr. Ann Cavoukian, Executive Director of the Privacy and Big Data Institute at Ryerson University, Three-term Information and Privacy Commissioner of Ontario, Creator of Privacy by Design

Privacy principles of PIPEDA as a benchmark

- ❑ **Principle 1 – Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
- ❑ **Principle 2 – Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
- ❑ **Principle 3 – Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
- ❑ **Principle 4 – Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
- ❑ **Principle 5 – Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
- ❑ **Principle 6 – Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
- ❑ **Principle 7 – Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- ❑ **Principle 8 – Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- ❑ **Principle 9 – Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- ❑ **Principle 10 – Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

CDI Strategic Governance Structure



CDI teams are consulting F/P-Ts and leveraging ESDC internal PMO Governance