



Government  
of Canada

Gouvernement  
du Canada

# CANADA'S DIGITAL INTERCHANGE (CDI) HIGH-LEVEL BUSINESS CASE

**Joint Councils**

Status	Final
Date	2016-08-30
Classification	UNCLASSIFIED

Canada

*This page left intentionally blank.*

## TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	5
1. WHAT IS CANADA'S DIGITAL INTERCHANGE?.....	12
1.1. CORE FUNCTIONALITIES.....	13
1.2. CDI WITHIN THE PAN-CANADIAN TRUST FRAMEWORK .....	17
1.3. EVOLUTION TOWARDS CDI.....	18
1.4. VALUE PROPOSITION FOR CDI.....	20
1.5. BENEFITS REALIZATION .....	23
1.5.1. DIRECT COST AVOIDANCE .....	23
1.5.2. INDIRECT COST AVOIDANCE.....	25
1.5.3. SERVICE IMPROVEMENTS.....	27
2. BUSINESS NEEDS .....	28
2.1. FEDERAL BUSINESS NEEDS .....	30
2.1.1. NOTIFICATIONS, VALIDATION AND RETRIEVAL DATA NEEDS .....	33
2.2. PROVINCIAL AND TERRITORIAL BUSINESS NEEDS.....	34
2.2.1. PT IDENTITY NEEDS .....	35
3. FEDERAL INFORMATION SHARING AUTHORITIES & PRIVACY .....	35
3.1.1. BROAD APPROACHES .....	36
3.1.2. TARGETED APPROACH .....	38
3.1.3. PRIVACY CONSIDERATIONS & ISA FRAMEWORK.....	39
4. GOVERNANCE - A PAN-CANADIAN APPROACH.....	42
4.1. OPERATIONAL OVERSIGHT AND MANAGEMENT .....	43
4.2. SERVICE PROVIDER OPTIONS .....	45
4.3. GOVERNANCE MODEL SUMMARY .....	49
5. ANTICIPATED COSTS.....	50
5.1. TECHNICAL COSTS .....	50
5.2. BUSINESS COSTS .....	54
5.3. PAYBACK.....	55
5.4. COSTING SUMMARY .....	55
6. PATH FORWARD.....	55
ANNEX A – GLOSSARY .....	57

ANNEX B – FEDERAL BUSINESS NEEDS SUMMARIES .....	63
ANNEX C – SUMMARY OF CURRENT FEDERAL AUTHORITIES .....	83
ANNEX D – TEN PRIVACY PRINCIPLES .....	84
ANNEX E – BEST PRACTICES - NATIONAL AND INTERNATIONAL EXAMPLES .....	87
ANNEX F – COSTING SPECIFICS.....	89

## EXECUTIVE SUMMARY

### *In the digital era, citizens' service expectations are evolving.*

Advances in digital technology have disrupted traditional service delivery models and have raised the bar in terms of what people expect when it comes to customer service. Citizens' expectations are being shaped by high-quality service experiences provided by leading private-sector companies. Banks allow clients to quickly check balances, transfer funds and pay bills via mobile apps. Retailers offer a wide range of service delivery options and easy returns. In this new digital era where citizens' expectations of service are rapidly increasing, governments must rise to the challenge.

Around the world, governments are moving forward with efforts to improve service delivery. Canada is no exception. For the past decade, all levels of Canadian government have launched initiatives to modernize service delivery to meet citizens' expectations and reduce costs. At the center of these efforts is the move toward an improved digital service experience.

### *CDI is part of the government response to provide better digital services.*

In Canada, identity management is a shared domain among federal, provincial and territorial (FPT) governments. For instance, provinces and territories have jurisdiction over vital statistics which include births, deaths and legal name changes while the federal government is responsible for the information on the legal status of residents born abroad and the social insurance number.

Identity validation and management are central points for service delivery. Yet, in Canada, this function remains locked in a non-digital domain and it has become a significant barrier to implementing digital service transformation.

Canada's Digital Interchange (CDI) is the key enabler for better digital government services. By providing a set of standards, information-sharing agreements, and technical infrastructure, CDI aims to enable government systems to securely and efficiently exchange, validate and update identity information in real-time, allowing for a seamless quality service experience for clients. CDI will support the implementation of a Tell-Us-Once approach and will enable multijurisdictional and multi-sector service bundles, similar to the existing Newborn Registration Service. This will significantly contribute to improving digital services to Canadians while maintaining the integrity of government programs and services.

CDI has three key tenets:

1. To protect personal information through standardized and comprehensive approaches in order to ensure security, minimize risk of data breaches and promote proper accountability of all partners.

2. To allow jurisdictions to confirm identity information and to exchange updated information where legal authority exists, through a secure and cost-effective technology solution.
3. To avoid redundancy and duplication by implementing a solution that does not create new databases or repositories of personal information.

### ***This business case strengthens the value proposition of CDI***

This high-level business case for CDI was prepared by the federal Treasury Board Secretariat and the Department of Employment and Social Development Canada, in collaboration with the CDI Federal Operations Committee and the FPT Project Oversight and Coordination Committee. The business case responds to a request from the Deputy Ministers Committee on Service and Federating Identity in August 2015. The purpose of this business case is to confirm CDI's scope, value proposition and business needs, and to examine options for a way forward.

The business case includes background information on the CDI initiative and explains its core functionalities, the relationship with the Pan-Canadian Trust Framework, the key value proposition and the expected benefits. Federal, provincial and territorial business needs addressed by CDI are discussed in detail as well as key legal and privacy considerations related to information-sharing.

Many aspects of this document have a strong federal focus. Hence, this business case should be considered partial until it can fully incorporate input from PT partners. The aim is that with continued FPT engagement and collaboration, the full vision for a pan-Canadian initiative will be realized.

### ***CDI addresses key business needs at the federal level***

CDI responds to the need for a scalable, interoperable and secure identity validation system with access to multiple authoritative sources across Canadian jurisdictions. This need is evident at the federal, provincial and territorial levels.

At the federal level, CDI has been identified as the enabler and/or driving force behind key programs and services. Specifically:

- **Supporting Program Integrity** – Departments and agencies rely primarily on the security of their systems and processes for delivering benefits and services. They all require varying degrees of assurance to confirm the identity of individuals. A number of service offerings rely on their internal departmental ecosystem to support program or service integrity as they relate to identity.
  - *CDI is seen as an enabler to facilitate the expansion of authoritative data sources to authenticate program information against someone else's data for the purpose of service delivery.*

- **Supporting Evidence of Identity** – There is a general consensus that “foundational documents” issued by Vital Statistics Organizations for individuals born in Canada (e.g. birth certificates) and citizenship documents issued by Immigration, Refugees and Citizenship Canada for individuals born abroad (e.g. Certificate of Canadian Citizenship) or who have a legitimate status in Canada (e.g., permanent residence, work permit, study permit) serve as key proof that the identity claimed by an individual is legitimate and valid. Expanding access to this information to partners at all levels of government in a real-time setting will improve efficiencies while enabling involved stakeholders to reduce identity and benefit fraud.
  - *A number of federal departments and agencies expressed interest in validating identity against additional supporting evidence (e.g. federal and/or provincial and territorial authoritative sources) in order to increase the confidence level behind their online customer service channel without the need of in-person or out-of-band processes.*
- **Compliance with the *Policy on Identity Management*** – A number of departments and agencies linked their program need responses to ongoing efforts in implementing the Treasury Board Identity Management policy requirements.
  - *CDI can potentially enhance data integrity, reduce costs, eliminate inefficiencies and lower risk for error as stakeholders work to improve how departments authenticate and provide the legitimacy of identity claimed by clients.*
- **Common Data Exchange Standards** – Existing ad-hoc connections between departments and agencies and others need to be expanded to simplify or accelerate processes. Data exchange methods currently in place seemed to vary greatly between organizations and programs. Three departments (Employment and Social Development Canada, Canada Revenue Agency, and Statistics Canada) currently exchange birth and death information with 10 Provinces using a common data exchange standard. *A common standard will likely to be required in order for CDI to be an effective solution.* The Pan-Canadian Identity Validation Standard has been endorsed by the FPT DM Table on Service Delivery Collaboration. The Pan-Canadian Identity Information Exchange Specification has been drafted and endorsed by the Identity Management Sub-Committee.

The following specific business needs have been identified at the federal level. These needs were brought forward through a questionnaire that was sent to members of the CDI Federal Operations Committee in fall 2015:

- **Notification of a Birth or Death Event** – Ten of the eleven consulted departments and agencies identified the need to receive birth or death information from Vital Statistics Organizations in order to support programs and client service delivery agents. Specifically:
  - **Access to Programs and Benefits** - Birth and death notifications were flagged as important information to ensure a client or a next of kin is directed to the

appropriate program or benefits, thus ensuring that individual data is up to date and client eligibility and direct access is triggered following a life event.

- **Timely Notices** – Timely life event notifications are key in preventing benefit overpayments and reducing administrative costs associated with debt-recovery activities.
- **Client Data Upkeep** – Service delivery agents need to be notified automatically when a client changes a key data attribute with another partner (e.g. address change). This lessens administrative burden and lowers the risk of fraud and adjudication efforts.
- **Validation and Retrieval of data against provincial and territorial organizations** – Twenty one programs and initiatives were identified as requiring CDI to support the validation of data function with their programs or services against authoritative sources, including:
  - **Validation Through Retrieval to Complete Identity Records** – Retrieval is a form of validation where the relying party identifies an individual and asks a question about a client to receive supplementary information. Although not directly linked with the identity of an individual, this information exchange transaction type is needed in order to obtain supplementary data about individuals associated with a Business Number.
  - **Mailing Address Information as Supportive Evidence** – An individual's postal address is a key data attribute that programs often have to manage and which falls into supportive evidence linking an individual to a proven identity. While no official authority exists for this attribute, stakeholders highlighted specific government-issued documents such as PT Transport and Health Ministry cards as having supporting address data that is refreshed on a cyclical basis. Canada Revenue Agency's Individual Identification database and Elections Canada's National Register for Electors were also cited as additional databases that could support the retrieval function.
- **Data Collection Need** - Statistics Canada highlighted a unique business need linked with its general data collection and surveying mandate. CDI could support such a need over time through a combination of notifications and retrieval exchanges.

### *CDI also addresses key business needs of the Provinces and Territories*

In December 2015, a business needs questionnaire (similar to the one sent to CDI Federal Operations Committee members) was sent to members of the Project Oversight and Coordination Committee to formally collect needs and understand how each jurisdiction proposes to connect programs, business lines, Vital Statistics Organizations, and Service



Ministries to CDI. PTs were also asked to identify authoritative sources from jurisdictions that would help support them in their service delivery.

While responses to this questionnaire are ongoing, the answers received so far, in addition to information gathered through other engagement activities, highlight a number of key considerations to support the development of CD, namely:

- **Vital Events data** – Information-sharing of vital events data is essential for birth and death notification data (not only with the federal government but also between provinces and territories). PTs need this information due to migration from province to province. Employment and Social Development Canada currently uses this infrastructure to validate birth information for program delivery.
- **Revenue Generation** – Transaction fees are a key consideration for PTs involved with CDI. PTs currently receive transaction fees from the federal government in exchange for birth and death information from Vital Statistics Organizations. These transactions account for a portion of the core budget supporting these organizations. Some PTs have recognized that the addition of partners would potentially allow them to increase their revenue generation.
- **Various States of Readiness / PT Data Hubs on Identity** - The state of readiness of PTs varies greatly from one another. Preliminary efforts in coordinating identity data are already in place (e.g., Newfoundland and New Brunswick have established ad-hoc connections to exchange death information among each other, while British Columbia has set up a process to allow any province to access its death information). Some provinces, such as Alberta and Quebec, have already been working on hub technology to connect their internal stakeholders. Alternatively, Ontario has indicated that it is not considering building a hub, and as a result, the Ontario Vital Statistics Organizations and service ministries would likely connect directly to a CDI hub to exchange information. The Atlantic Provinces and the Territories have recognized that a regional hub may be the most efficient way to move forward.

Needs to support PT partners are being derived from a combination of what the federal partners identified as supportive data that could be shared with PTs as well as intelligence gathered from the interactions with PT service ministries and Vital Statistics Organizations. Two primary requirements have been identified as key element to support existing governmental programs across the country:

- **Access to Identity Data**
  - **Identity Linkages Project & Immigration, Refugee and Citizenship Canada Data** – The Identity Linkages Project business case, which is a pathfinder to CDI, has clearly identified that PTs would gain significant benefits from a direct connection to immigration data. A connection to this data would 1) improve program and

data integrity, 2) reduce the risk of fraud to individuals and 3) improve service delivery to Canadians.

- **Fraud Prevention and Program Integrity** - Given that program recipients are often from other jurisdictions, PTs service delivery can greatly benefit from access to life event data from other jurisdictions.
- **Other Possible Federal Authoritative Sources** – With the expansion of federal partners, there is a possibility that PTs may wish to gain access to new CDI data sources. Further engagement is required to confirm this assumption with each stakeholder.
- **Exchange of Death Events between PTs**
  - **PT to PT Data Exchange** – CDI will need to enable PT to PT information-sharing. Labour mobility has constant impact on programs and services delivery. A successful CDI will allow PTs to access death information in a more rapid fashion.

### *To be successful, CDI requires changes to information-sharing authorities and common privacy protection practices*

While many federal departments have the necessary authorities to collect, use and disclose personal information for the purposes of CDI, some changes and clarifications in legal authorities are required to increase transparency and efficiency and to reduce risk. Additionally, the wording in some departmental legislation (e.g., *Citizenship and Immigration Act*) limits the collection, use and disclosure of information to physical documents as it requires clients to “present, provide or show” documents, which insinuates being physically present. This language needs updating to allow for information to be collected, used and disclosed electronically.

The business case recommends a broad approach to providing federal departments and agencies with the necessary information-sharing authorities to participate in CDI. This approach would include amendments to the *Privacy Act* and/or the development of a new stand-alone *Service Delivery Act* to provide the necessary authorities to enable digital services.

CDI aims to develop a multilateral Information-Sharing Agreement (ISA) framework that would consist of 1 Federal ISA (for information-sharing among federal partners) and 13 PT ISAs (for information-sharing between the Federal ISA and each of the PTs). This framework will eventually replace the over 650 existing bilateral ISAs and will ensure that all CDI parties are bound by the same information-sharing and privacy protection standards.

### ***A sound Pan-Canadian governance structure and financial model will also be essential to the success of the initiative***

To be successful, CDI needs to adopt a governance approach that supports the shared jurisdiction over identity in Canada. The business case examines options and recommends a pan-Canadian governance model with a well-defined representation and accountability structure, including funding, delivery and operations. The FPT Deputy Minister Table on Service Delivery, with the support of the Public Sector Chief Information Officer Council and the Public Sector Service Delivery Council (the “Joint Councils”), will continue to play a key strategic oversight role for CDI.

With respect to a financial model for developing and operating CDI, the business case explores technical and business requirements and associated costs, and presents options and considerations for further decision. Costing options will depend on future negotiations with FPT partners and on the governance model that is selected.

### ***The path forward***

The process of developing this business case confirmed the need for CDI as a scalable, interoperable solution for secure identity validation, notification of identity data changes, and retrieval of identity-related data among Canadian FPT partners. CDI will enable all jurisdictions to deliver a better digital service experience and will thus provide benefit and value to Canadians.

Further collaboration with PT partners is required to move forward with CDI. The existing CDI governance structure can be leveraged for this purpose to seek endorsement and commitment to continued collaboration on the outstanding design elements, governance and financial models and other key decisions.

In parallel, the federal government will continue advancing strategic elements related to information-sharing authorities (as outlined in this business case) and the development of a federal infrastructure. These efforts will be done as part of the development of the Government of Canada’s Client-First Service Strategy.

## **1. WHAT IS CANADA'S DIGITAL INTERCHANGE?**

CDI is a key enabler for digital services. It will consist of standards, information sharing agreements and infrastructure to allow real-time, scalable, cost-effective service that will enable both levels of government to securely confirm an individual's identity information to support online service delivery. The initiative has three proposed key objectives:

1. Standardized and comprehensive approaches for the protection of personal information, in order to ensure security, minimize risk of data breach and appropriate accountability of all partners.
2. Implement a secure and cost-effective technology solution that will allow jurisdictions to confirm identity information, and provide updated information where legal authority exists to do so.
3. Implement a solution without creating any new databases or repositories of personal information.

CDI would enable government systems to communicate with each other to validate that identity information of an individual is accurate. As well, it would allow parties to notify each other when identity information has changed so that an individual need only tell one department/agency in one level of government of a change and all others would be told in near real-time (e.g. death notification).

While the focus of CDI upon initial launch would be to connect federal and provincial governments to one another, future partners could include municipalities as well as organizations from the private sector (banks, NGOs, etc.). Provinces have indicated that municipalities should be considered a key partner in using the Pan-Canadian approach to exchanging information. Business needs for future partners have not been determined at this point.

For the past decade, there has been a concerted effort by both levels of government in Canada to improve service delivery while reducing costs. The central focus of this strategy has been to move services online, allowing Canadians to make every day, low risk transactions with their governments more convenient.

Identity management is a shared domain in Canada. The provinces and territories have jurisdiction over vital statistics which includes births, deaths and legal name or sex changes of citizens born in Canada. The federal government has jurisdiction related to legal status of residents born abroad (e.g. citizen, permanent resident, temporary foreign worker). Canada's governments must work even more closely together if they wish to confirm that identity information is accurate and offer seamless services to citizens.

Given the shared identity domain CDI will be designed to support a pan-Canadian approach to exchanging identity information between key partners, including:

- federal departments/agencies;
- provincial and territorial governments and federal departments/agencies; and

- provincial and territorial governments, which could also exchange information amongst themselves.

CDI supports a “Tell Us Once” approach and could enable multijurisdictional and multi-sector service bundles, similar to the existing Newborn Registration Service. For example, when an individual passes away, the next of kin could inform both levels of government, banks and other entities (e.g. a pension plan or insurer) at the same time. This would improve services to Canadians, while at the same time maintaining the integrity of government programs and services.

## **1.1. CORE FUNCTIONALITIES**

There are three core CDI functionalities for programs and business lines available to participating departments and agencies to share information: validation, notification of a change in personal information and retrieval of data.

### **NOTIFICATION**

Notification is the act of disseminating information about a change in personal information based on a life event. The following vignette illustrates how an event in a PT can trigger a number of notifications to relying federal and PT partners.



John just passed away at the age of 74. He was a retired veteran who lived in Victoria, BC. At the time of his passing, he was receiving the Canada Pension Plan (CPP), Old Age Security (OAS) as well as additional support from Veterans Affairs Canada for his military service (disability benefits).

Dealing with the death of a loved one is difficult and settling affairs can be a challenge. Typically, a family member has to inform a number of local, provincial and federal programs as well as private institutions of the passing.

*CDI supports the establishment of "Tell us Once" initiatives to help Canadians through the system.*

John's daughter, receives a **Medical Certificate** from the hospital and provides it to a funeral director who registers the death with the Vital Statistics Office (VSO) by completing a **Statement of Death**.

In BC, the Vital Statistics Branch is responsible for **registering a death** and providing the official **Death Certificate**.

The BC VSO/SM issues a **Death Certificate** containing the following information:

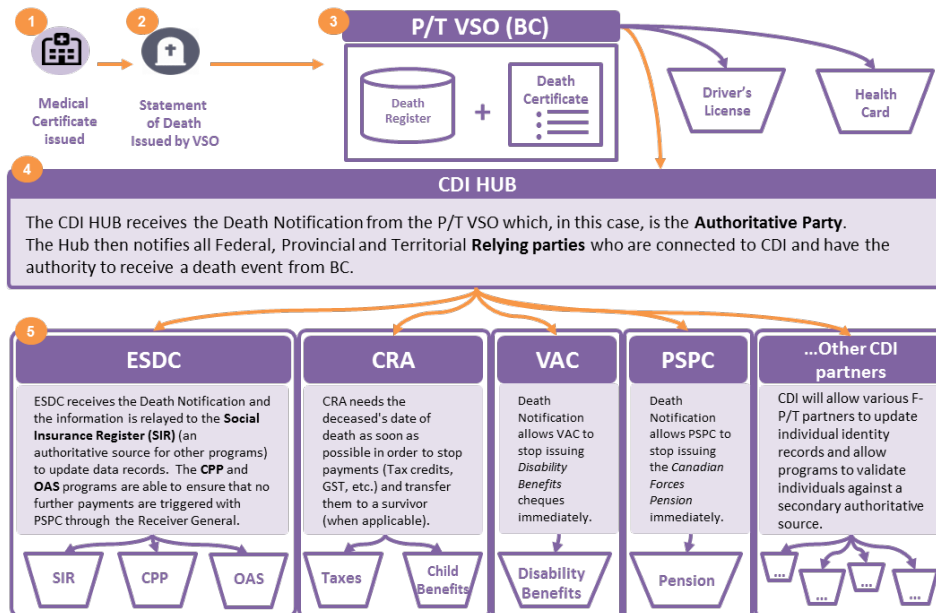
- Name of the deceased
- Date of death
- Place of death
- Date of birth
- Province or country of birth of the deceased
- Registration number
- Registration date of death
- Date issued of certificate

The P/T then shares this information with other provincial Transport and Health arms to cancel John's *Health Card* and *Drivers license*.

A **DEATH NOTIFICATION** is triggered in the CDI HUB from **the Authoritative Party** (P/T VSO) to automatically inform the various **Relying Parties**.

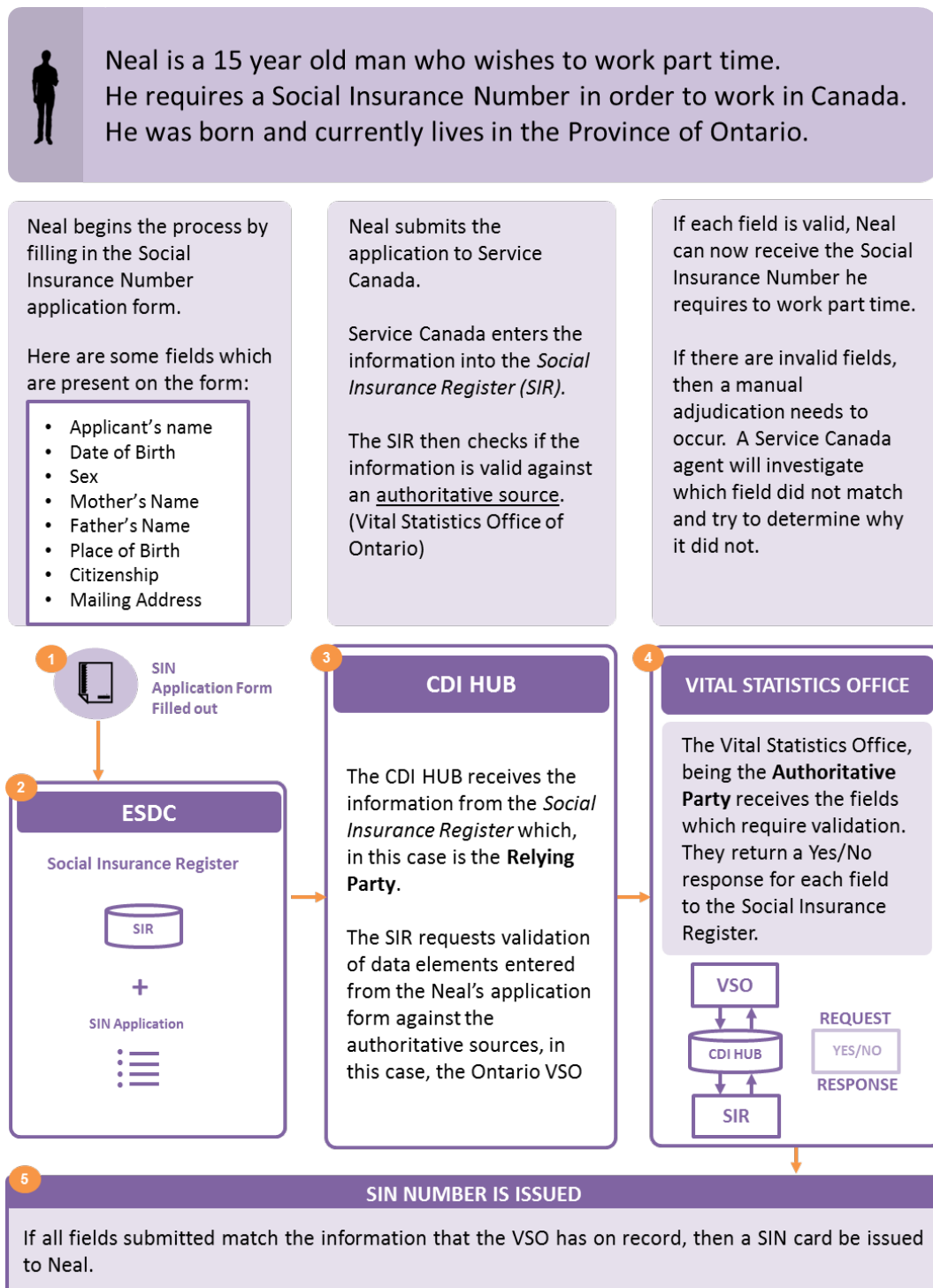
A number of federal programs are in need of this information to update their records and some may need to perform an action (change in status, stop a payment, etc.).

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).



## VALIDATION

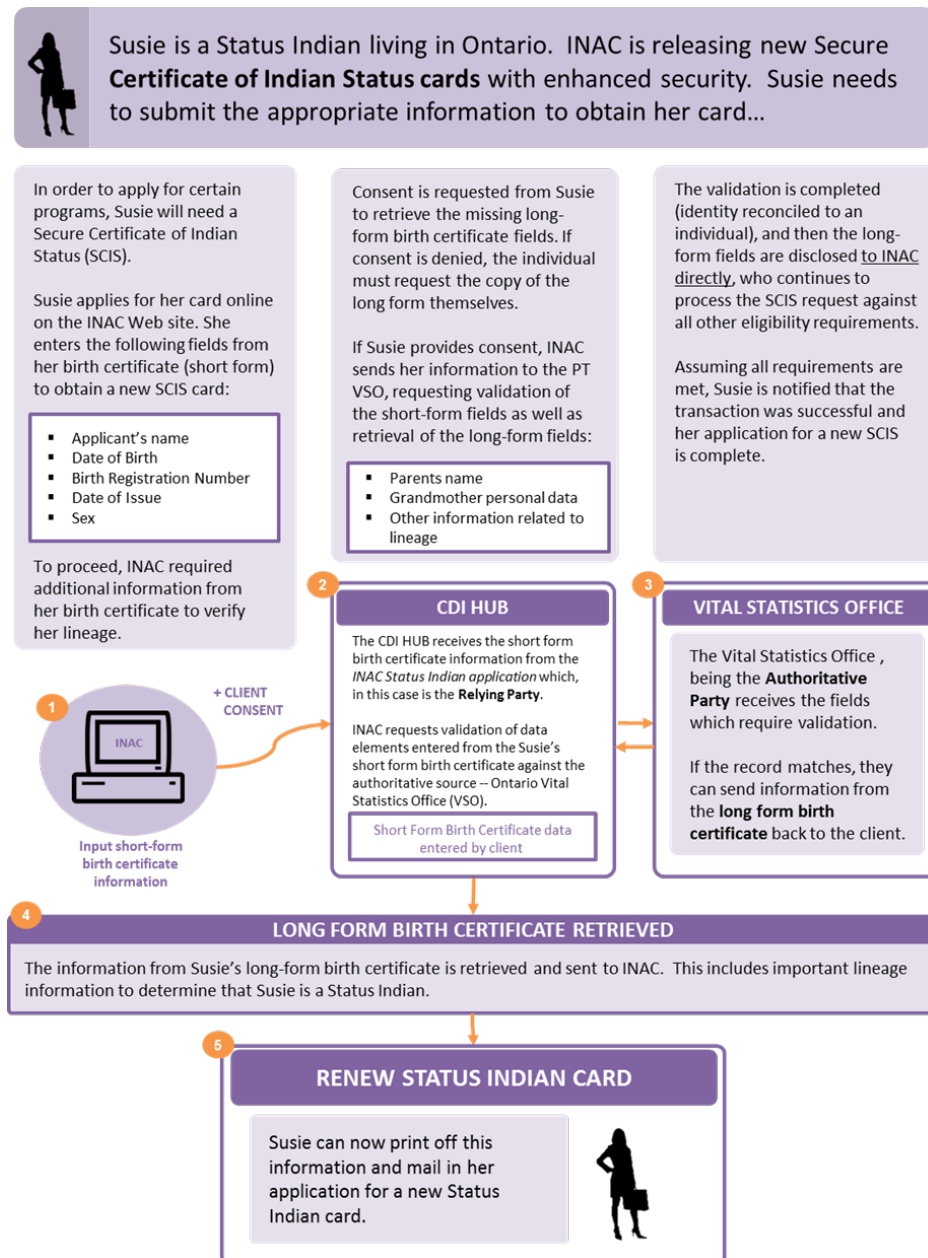
This function allows for the validation or confirmation of personal identity information against an authoritative source. The following vignette illustrates how a federal program could use CDI to validate data with a PT database.



Note: If no match is made, a business process (adjudication) will occur outside of CDI.

## RETRIEVAL

The retrieval function is a form of validation. A retrieval of personal identity information involves identifying an individual and seeking additional data that is critical to a program or business process. The following vignette illustrates how a federal program could request additional information from a PT to process a citizen request in a program.



It is important to note that jurisdictions will need to determine if their current legal authorities allow them to use any/all CDI functionalities. For example, Alberta has indicated that while they can see a use for the Notification and Validation functions, they do not see a value in having a



retrieval function and further to that, current provincial legislation related to access to citizen data maintained by Motor Vehicles, Health, etc. would not allow a retrieval function to proceed without significant changes.

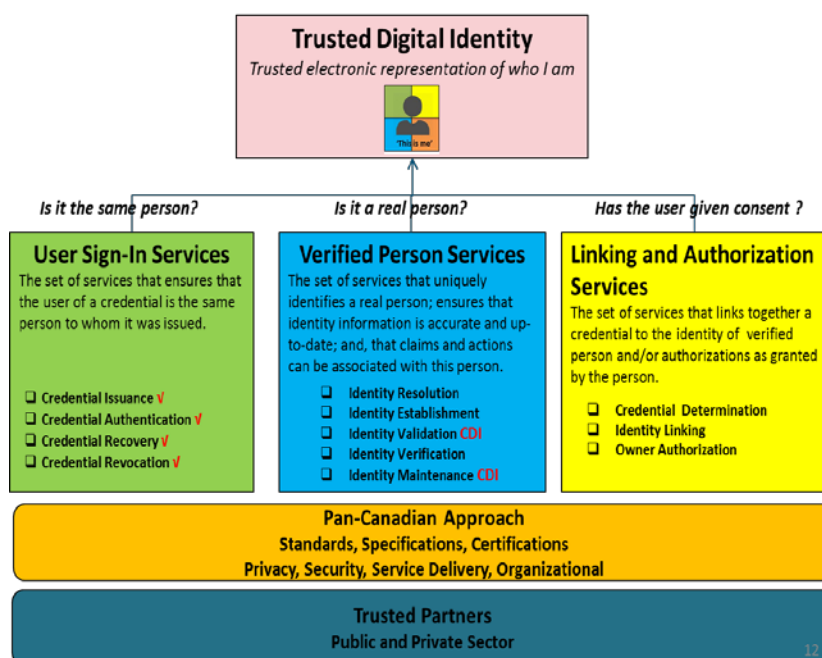
## 1.2. CDI WITHIN THE PAN-CANADIAN TRUST FRAMEWORK

To deliver services, governments need to know that citizens are who they say they are. In the physical world, organizations rely on documents issued by governments to prove identity. These documents have embedded security features and are trusted by other governments.

As Canada moves towards strengthening digital service delivery, documents cannot be relied on to provide assurance of identity; an electronic means of establishing identity is required to facilitate online transactions.

As individuals move across the country throughout their lives, they will want to access digital services with minimal interruption. Canada's governments need a way to trust identity information that travels over jurisdictional boundaries and find ways to ensure information remains up to date. With trusted, real-time digital identity management, a broad suite of digital services for Canadians can be offered.

The *Pan-Canadian Trust Framework* has been endorsed and approved by the Identity Management Steering Committee (IMSC) under the Joint Councils<sup>1</sup>. The Framework ensures that identity management business processes have the necessary integrity and that the exchange of identity information is standardized in a manner to enable interoperability across jurisdictions. This is achieved by defining the common rules, processes and standards to which everyone has agreed, driving towards a trusted digital identity that can be relied on across the many jurisdictional and organizational boundaries within Canada. The end objective is that each citizen has a trusted digital representation of themselves that is secure, or more so, than if they appear in person at a service desk with documents. CDI would support the validation and maintenance portions of the Identity Trust Framework.



<sup>1</sup> The Joint Councils is comprised of the Public Sector Service Delivery Council (PSSDC) and the Public Sector Chief Information Officer Council (PSCIOC). Jointly, these organizations steer sub-committees aimed at areas of interest to both the service delivery and CIO communities.

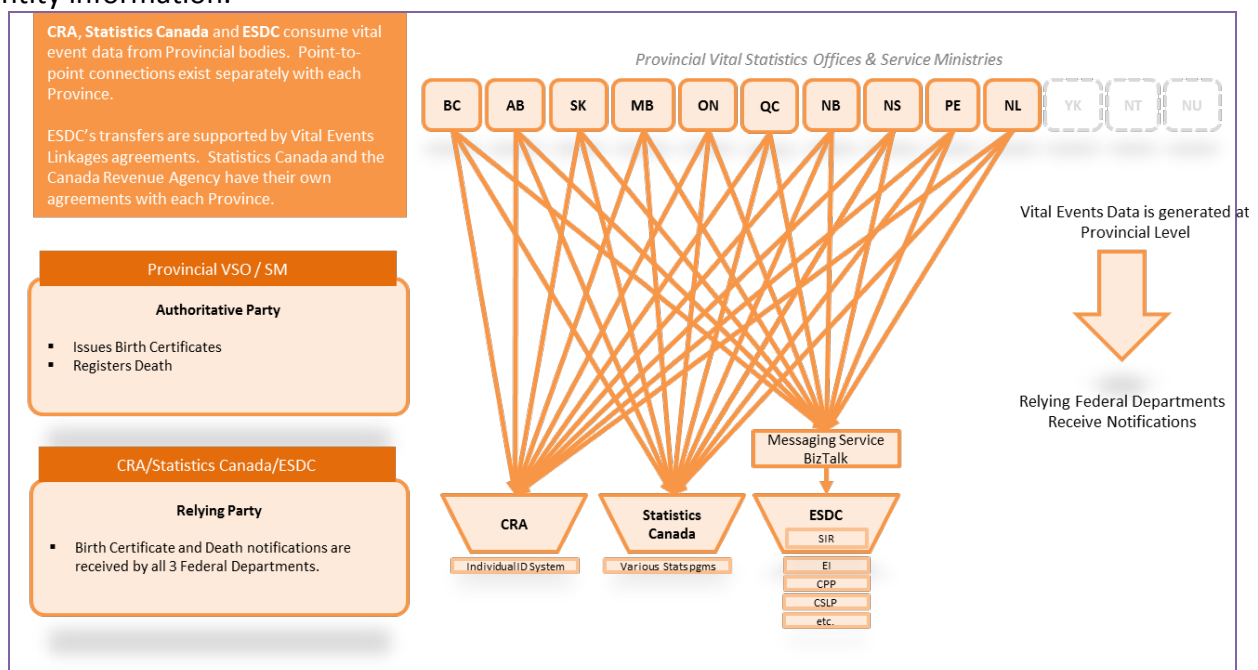
However, it is important to note that some jurisdictions may choose to always require some form of in-person identity verification in order to create a Trusted Digital Identity.<sup>2</sup>

### 1.3. EVOLUTION TOWARDS CDI

The GC introduced a number of mandatory policy instruments for departments/agencies, such as the *Directive on Identity Management (2009)* and the *Standard on Identity and Credential Assurance (2013)*, to ensure consistency and interoperability in identity management practices. These policy instruments are based on the *Pan-Canadian Assurance Model*, a proposed model for moving towards federated identity in Canada to support digital service delivery.

#### VITAL EVENTS VIA NATIONAL ROUTING SYSTEM (NRS)

Launched in 2004, the NRS currently connects three federal departments/agencies (CRA, ESDC and Statistics Canada) to provincial vital statistics offices. The NRS has led to the strengthening integrity of key federal programs. But, these bilateral exchanges do not allow for the efficient expansion of these connections to support information exchanges between all federal and provincial departments/agencies that need to validate, retrieve or receive notifications about identity information.

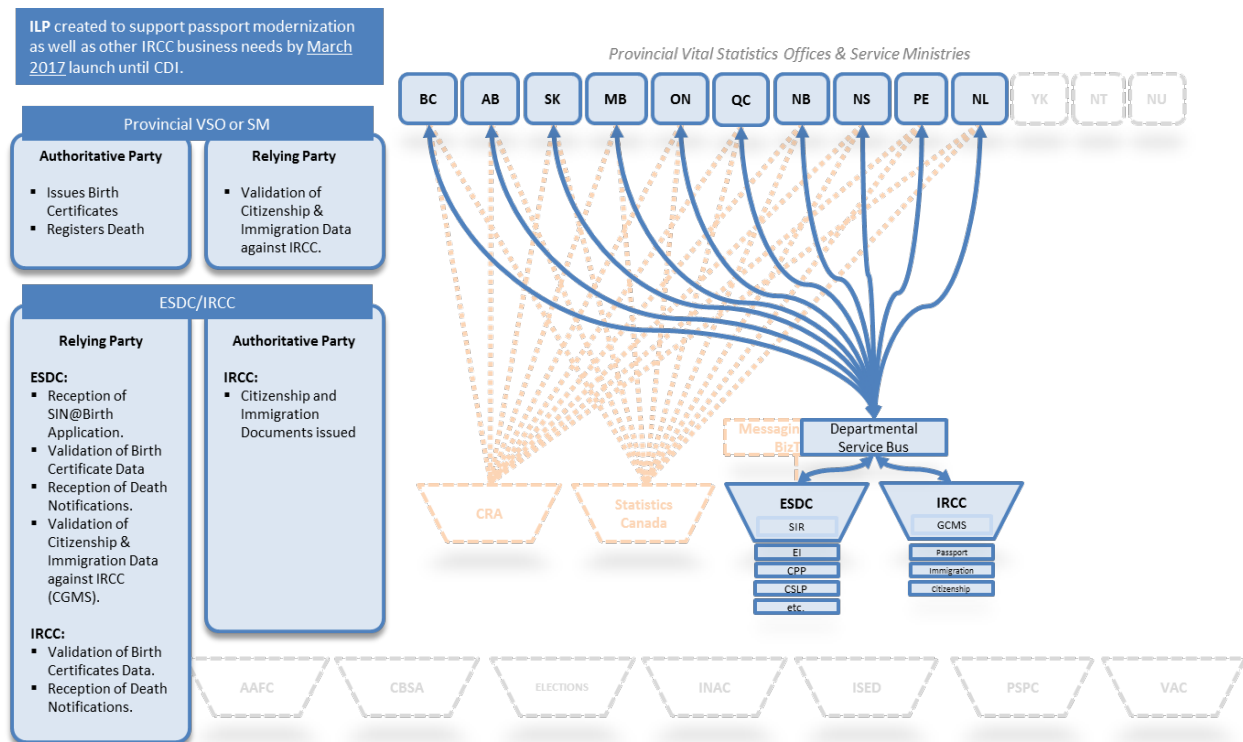


#### IDENTITY LINKAGES PROJECT (ILP)

The ILP is intended to be a pathfinder for CDI. ESDC and IRCC established this project to support passport modernization through the electronic validation of identity information. A key reason for doing so was accelerated timelines to deliver on the initiative before CDI would be fully operational. Under ILP, one of the proposed key elements that will inform the on-going

<sup>2</sup> Government of Alberta initial feedback indicated this point.

development of CDI is the migration of technology towards a single service bus or hub, moving away from bilateral, point-to-point connections.



## CANADA'S DIGITAL INTERCHANGE

The evolution forward to CDI will build on the concept of the secure sharing of identity information through a common information exchange model. While the technical architecture of CDI is being determined, the vision is a single data exchange model, ensuring that the necessary information is shared with appropriate partners at the appropriate time. The following graphic is for illustrative purposes only and does not reflect what the final technical architecture will be. It is important to note that while the technical architecture is one challenge, a potential large challenge is to ensure proper authorities are in place to exchange information between governments.

CDI will be a *real-time, scalable, cost-effective* service that will enable all levels of government to securely confirm identity information to support enhanced digital service delivery.

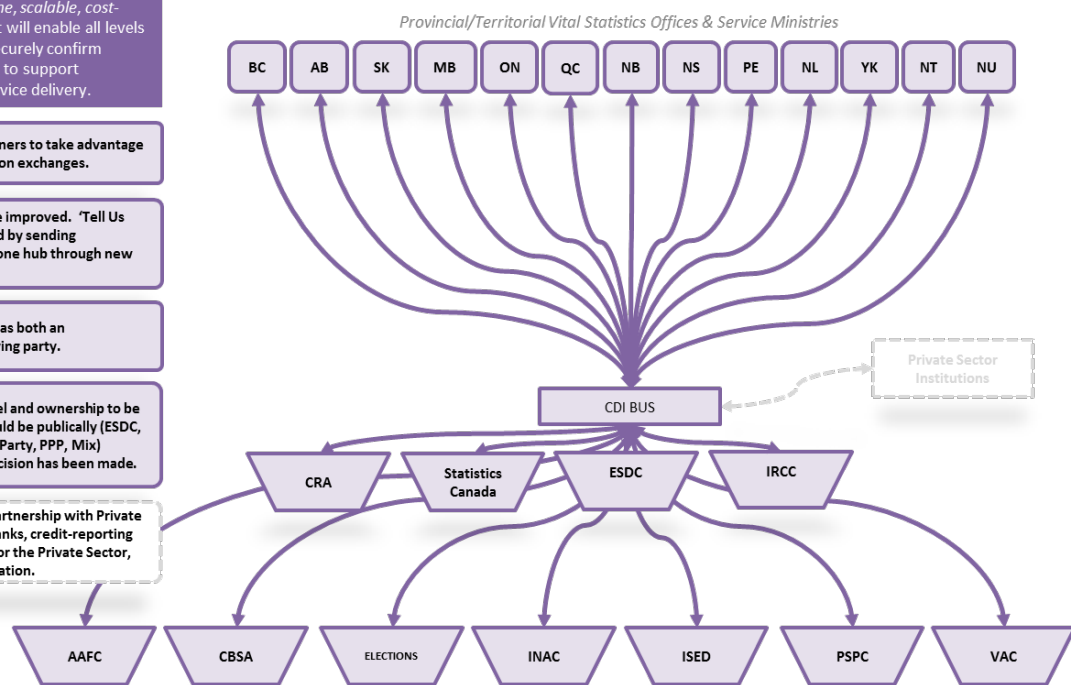
CDI Allows more partners to take advantage of common information exchanges.

Digital services can be improved. 'Tell Us Once' can be achieved by sending information through one hub through new authorities.

CDI members can act as both an authoritative and relying party.

CDI governance model and ownership to be decided. CDI Hub could be publically (ESDC, SSC) or privately (3rd Party, PPP, Mix) administered. No decision has been made.

Potential for future partnership with Private Sector Institutions (banks, credit-reporting agencies, Validation for the Private Sector, etc.) for Identity validation.



## 1.4. VALUE PROPOSITION FOR CDI

In the digital era, Canadians have high standards for the service they receive and dealing with governments should be no exception. Canadians deserve high-quality services delivered in a way that is immediate, accessible and responsive to their needs, and with confidence that their personal information will be protected. These objectives are sometimes not easily reconcilable.

There are many examples of governments taking action to develop and implement strategies and solutions targeted at improved service experiences and modernization towards digital service delivery:

- The federal government made a commitment in Budget 2016 to take action to make it easier to access services government online and to establish new performance standards for federal services.
- The ServiceOntario Strategic Plan advances an ambitious service agenda and includes the creation of a digital service office, led by a chief digital officer, to drive change.
- British Columbia has the *Citizens@The Centre* strategy that includes increased citizen engagement and self-service, use of telepresence technology, and effective and secure identity management.
- In Nova Scotia, the Digital Service department is responsible for the transformation of digital services across government and delivering online services including creating, enhancing, and maintaining websites and transactional services.

- The Government of Alberta has had many accomplishments in regards to work being done in digital identity:
  - Alberta has been live with their digital identity program since July 2015.
  - Alberta is the only province that links credential and identity and passes both credential and identity attributes in the SAML assertion that is sent to relying parties.
  - Alberta has modified the federal government's CATS2 specification to allow both credential and identity attributes to be passed in a SAML assertion.
  - Alberta is currently completing an implementation of the Level 3 verification process for our citizens to be able to get to a level 3 identity assurance level and during this process have implemented a version of the CDI hub in order to validate driver's license information with our Motor vehicles database, and will be implementing the same functionality to validate birth certificates with Vital Statistics in the near future.
  - Alberta believes they are a leader in the digital identity field and the province has offered to do pilot projects with the federal government such as passport renewals online.
  - Alberta was instrumental in helping to develop a working version of the Identity Validation Standard.

CDI will be a set of standards and infrastructure to facilitate the secure exchange of identity information in real time. It is important to be note that while CDI enables digital services to mature and grow, CDI in itself is not the direct mechanism which will create service improvements. For service improvements to happen, FPT departments, agencies and organizations have to make changes to their systems to best leverage real time identity validation.

CDI is designed to facilitate improved service to Canadians by allowing governments to securely and efficiently exchange identity information in real time. The value proposition for CDI has three main pillars:

1. improved service experience for individuals;
2. improved service experience for business by bringing more programs and services online and integrate towards a "tell us once" approach; and,
3. promoting confidence to citizens that privacy safeguards are in place to ensure personal information is handled fairly and transparently.

## **1. TELL US ONCE – SERVICES TO INDIVIDUALS**

In June 2013, the Clerk of the Privy Council launched Blueprint 2020 with the aim of continuing to build a more open and networked federal public service that improves the lives of Canadians while enhancing systems and practices and better using information and ideas. One of the key elements of the initiative, the "smart use of technology" theme focuses, among other topics, on

establishing e-enabled and seamless services providing for “Tell Us Once” information gathering. Cost-effective solutions capable of reducing duplication and fraud were identified are needed to allow Canadians to interact with their government in an easier fashion.

As an example, since 2010, the Province of Québec has been using a “Tell Us Once” method for birth and death notifications and changes to name/sex. They send these notifications to 16 different departments/agencies within the province as well as notifications to the federal government.

Using CDI as the mechanism for real time validation of identity information, FPT departments, agencies and organizations could allow Canadians to make changes to their personal information online knowing that those changes will be communicated to other relevant departments. Canadians could make these changes on their own schedule, at their convenience, reducing the need for in-person visits to service centres.

## **2. INTEGRATION WITH BUSINESS NUMBER – SERVICES TO BUSINESS**

CDI has also has value for Canadians who own their own businesses. CDI is envisioned to not only aid citizens, but businesses as well. It is important to note that this is not planned as an initial function within CDI. An initiative is underway to harmonize business identification across the federal government, provinces, territories and municipalities by having all jurisdictions and programs use the CRA Business Number (CRA-BN) as the common business identifier throughout government. The Province of Québec has indicated that they may not wish to use the Business Number as the common business identifier, but they are not opposed to adding it to its registries.

Before an individual can be associated with a business, their identity must be validated so the government can be reasonably assured that the individual is who they say they are. CDI could be used as the infrastructure for this step of the process, which could ease the authorization process for business owners and the federal government.

As CDI matures, linkages to the Corporate Registry within provinces will be explored along with additional uses for businesses. Corporate Registries are the entities which look after businesses in the provinces, in the same manner that Vital Statistics looks after citizens.

## **3. STRENGTHENING INFORMATION SHARING PRACTICES**

A single pan-Canadian identity validation service would strengthen privacy practices by moving from a less secure paper-based validation process to an electronic system.

Moving identity validation efforts from physical (e.g. paper, USB key) to electronic formats could reduce risks of security breaches around personal information. There is also limited ability to detect access. Canadians trust in the systems and protective mechanisms introduced to date; the maintenance of this trust is vital to the success of this initiative.

A 2013 PricewaterhouseCoopers poll<sup>3</sup> of over 3,000 Canadians on government e-services found that 81% of respondents<sup>4</sup> were at least somewhat comfortable with the government validating identity online. Further, a majority<sup>5</sup> of respondents were comfortable with government organizations sharing basic identity information (name, address, date of birth) with each other in order to provide services. Therefore, we can assume there is evidence that Canadians would support increasingly automated, online identity validation services to reap the benefits of convenience these services would provide.

That said, just over half of respondents felt that privacy protection was the most important concern when it comes to government eservices<sup>6</sup>, underscoring the importance of designing a next-generation identity validation service with privacy considerations embedded.

The status quo, with its myriad of information sharing agreements poses a probable risk to Canadians' privacy rights. The eligibility rights of citizens are at risk by incorrect information contained within multiple databases if it is erroneously captured. Using the notification functionality proposed by this initiative, the inconsistencies between personal information banks would be greatly reduced.

## **1.5. BENEFITS REALIZATION**

The framework for benefits realization is outlined below, and is comprised of three distinct categories:

1. direct cost avoidance (e.g. those costs that can be eliminated or avoided by the business transformation processes as the result of using CDI);
2. indirect cost avoidance (e.g. those costs that can be avoided or recovered by improved sharing of identity information attributes); and,
3. overall service improvements (e.g. non-quantifiable benefits).

This framework has been populated with several illustrative examples, and further work will be undertaken to more fully attribute these benefits with engagement by all partners. It is important to note that, in large part, the benefits realized will be at the program level of the participating jurisdiction.

### **1.5.1. DIRECT COST AVOIDANCE**

Although CDI requires an initial upfront investment, federal departments/agencies could realize a number of long-term savings with this initiative. ESDC's EI Program could use CDI to gain access to additional authoritative sources of data in order to validate identity (e.g. VSOs). This

<sup>3</sup> PwC Citizen Compass on the Next Generation of Government eServices: <http://www.pwc.com/gx/en/psrc/canada/citizen-compass-the-next-generation-of-eservices.jhtml>

<sup>4</sup> 24% were very comfortable, 30% comfortable and 27% somewhat comfortable.

<sup>5</sup> Responses depended on what information is being shared. For example, 84% of respondents were at least somewhat comfortable with their name being shared, compared to 65% for a driver's license or passport photo.

<sup>6</sup> PwC Citizen Compass on the Next Generation of Government eServices: <http://www.pwc.com/gx/en/psrc/canada/citizen-compass-the-next-generation-of-eservices.jhtml>. p 5



would allow the program to eliminate sending access codes by mail, leading to an annual cost savings of \$2M<sup>7</sup>. Access to additional authoritative source of identity would reduce errors and could improve the overall accuracy and stewardship over payments. For example, OAS would be able to close a citizen's record faster upon notification of death. When overpayments occur, the time and effort dedicated to contacting citizens, correcting errors and resolving files could be achieved more quickly. This could also reduce volume of in-person service to citizens due to improved online services.

## REDUCTION OF IN-PERSON CHANNEL

As secure identity validation becomes a reality, online services will increase.

PriceWaterhouseCooper reports that online usage dominates and will continue to grow while traditional channels (telephone, in-person and mail) continue to be used, but the frequency of usage is expected to decline<sup>8</sup>. Savings can be realized as more in-person services shift to the online channel. It is important to note that while in-person is reduced, call center volumes go up significantly when new changes are implemented. The Office of Auditor General of Canada produced an audit on Access to Online Services which indicated per-transaction costs among 11 selected departments were:

- An online transaction costs the Government \$0.13
- A telephone transaction costs \$11.69 (90 times more expensive)
- An in-person transaction costs \$28.80 (222 times more expensive)

Having a government-wide strategy for service delivery can result in significant savings, including a reduction on staffing to support "in-person" service channels (e.g., reduction in required resources in larger Service Canada centres).<sup>9</sup>

## ADMINISTRATIVE OVERHEAD OF INFORMATION SHARING AGREEMENTS

Information sharing agreements (ISAs) detail restrictions on the use or disclosure of information that is shared from one department or ministry to another. While this may act as a privacy protection, it also means that the current assortment of ISAs may be an impediment to reaching a more efficient solution. Individual ISAs currently in place require human resources to maintain and renegotiate. It is difficult to determine the exact cost of negotiating an identity ISA in particular. As these ISAs are integrated into program delivery, negotiation and implementation costs are subsumed under overall program costs in departments' Program Activity Architecture. One consequence of identity validation being de-centralized into programs is the inability for costs to be precisely identified.

Overall estimated costs of negotiating an ISA ranged from \$73K to \$85K per department (this does not include O&M, legal services and IT expertise). This assumes that it took on average,

---

7 Michelle Seaton (EI) : In 2015/16, approximately 2.7M EI applications were received via Appliweb (EI Online Tool clients use to apply for benefits, this tool is located outside of MSCA) x 0.75 cents per mailing

8 PriceWaterhouse Cooper Report: <http://www.pwc.com/gx/en/psrc/pdf/citizen-compass.pdf>

9 OAG 2013 Audit: [http://www.oag-bvg.gc.ca/internet/English/parl\\_oag\\_201311\\_02\\_e\\_38796.html](http://www.oag-bvg.gc.ca/internet/English/parl_oag_201311_02_e_38796.html)



four FTEs (at 25% of their workload) approximately one year to negotiate an ISA, whether between federal departments or between federal and P/T entities.

A revised approach to information sharing agreements could have significant long-term savings for CDI. Having a multi-lateral ISA between federal departments and PT partners would reduce the number of individual ISAs in place.

## 1.5.2. INDIRECT COST AVOIDANCE

### IMPROVING IDENTITY DATA INTEGRITY

The inability to consistently validate identity against a number of authoritative sources has left all levels of government agencies vulnerable to error and fraud, resulting in the potential for overpayment of benefits and the issuance of genuine identity documents to fraudulent identities.

While there are a wide variety of identification documents and security features, not all service delivery agents have all the tools (e.g. an ultraviolet light reader) or the right training, to use all the security features on an identity document. Too often, criminals are easily able to use vulnerabilities and replicate less-secure documents, using them to obtain authentic documents with stronger security features. The result is so-called “synthetic identities,” identities that are artificial, which can be used to defraud individuals, governments and the private sector.

In the federal context, there are numerous smaller programs that would benefit from identity validation. Provision of agriculture funding programs such as AgriStability by Agriculture and Agri-Food Canada (AAFC) would benefit from having an increased level of assurance that the person applying is eligible. Public Services and Procurement Canada (PSPC) can benefit from real-time death notification to stop benefit payments to deceased public servants and make the process of obtaining survivor or child benefits more efficient. Veterans Affairs Canada would benefit in a similar fashion for its constituency.

On a more general scale, the Canadian Anti-Fraud Centre reports that, in 2015, more than 17,000 Canadians reported being victimized by identity fraud and losses totaled \$10.7M. This not only has financial consequences for Canada but can pose a risk to security. The ability to validate information in real time can also ensure governments record the right information about people, and can provide timely access to benefits and services to individuals. Of course, not all identity-related overpayments are due to fraud; they can occur due to an accidental failure to notify of a change in status in a timely manner or simply a clerical error.

In the period 2012-2014, 57,194 people were victims of identity fraud. In 2012 alone, losses totaled \$16M<sup>10</sup>. Also, each victim spent on average \$1200 to repair damage as a result of

---

<sup>10</sup> <http://www.antifraudcentre-centreantifraude.ca/reports-rapports/2014/ann-ann-eng.htm#a28>

identity theft and 30 hours of time resolving problems<sup>11</sup>, a total of \$68.6M dollars in direct losses for Canadians and 1.7 million hours of effort spent resolving identity fraud-related problems (from 2012-2014). This does not include the social and personal effects identity fraud has on individuals and their relation to other organizations, including the federal government.

## **TWO-FACTOR IDENTITY VALIDATION**

Introducing more authoritative sources to CDI allows for two-factor identity validation, which can improve the integrity of a service. For example, CRA, ESDC and VAC have specifically mentioned that they wish to use two-factor validation to authenticate an individual's identity prior to allowing access to online services.

In the case of Employment Insurance (EI), there is currently no immediate identity validation done when applying for EI as this would involve waiting for an access code to be mailed. Canadians applying for EI do not have time to wait for a letter to be mailed to them to continue an application. With the introduction of two-factor authentication, it introduces immediate identity validation.

The Province of Québec uses a similar type of authentication process when admitting permanent residents at the Montréal-Trudeau airport. Le 'Certificat de sélection du Québec (CSQ)' is compared with the official permanent resident documents and if there is no match, there is further investigations done by airport staff.

## **PASSPORT MODERNIZATION**

Under the Passport Modernization Initiative, IRCC and ESDC/SC are linking Service Canada's Vital Events Linkages (VEL) system and IRCC'S Global Case Management System (GCMS), as a means to strengthen security and integrity in identity management.

IRCC is undergoing a strategic transformation to bring efficiencies and improve the integrity of their programs. Electronic validation of identity document information is an important integrity measure, and is a key part of Service Canada's mandate for delivering the Passport Program within Canada. It can be accomplished by establishing linkages between Provincial (P) Vital Statistics Agencies (VSAs) or Service Ministries and IRCC.

IRCC and ESDC have been preparing the Identity Linkages Project (ILP) project proposal, which aims to establish a messaging system that will connect IRCC to VSAs or Service Ministries, via an ESDC messaging hub, with the intent of validating identity document information with the authoritative source.

## **OVERPAYMENTS**

---

<sup>11</sup> <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/archive-dntt-thft-rprt/index-en.aspx#a06>

CDI could be used to validate identity information and support program delivery and reduce instances of identity fraud. Governments have the opportunity, not only to prevent overpayments, but also the costs associated with recovering the overpayments once they are discovered. From the fiscal year 2011-2012, the Auditor General has determined that \$110M of overpayments is due to fraud<sup>12</sup>. Validating identity is one of the first steps in determining eligibility and preventing overpayments. With services such as health care, better identity validation processes can help ensure that limited resources are going to those who are entitled to them.

Last year, the Government spent approximately \$72.9 B in major transfers to persons through programs like EI, CPP and OAS. This figure does not include smaller transfers to specific populations, such as veterans or members of First Nations. It is difficult to estimate benefit overpayments with a high degree of accuracy, however even departmental estimates illustrate the scope of the problem. For example, Veterans Affairs Canada reported \$20.6 M<sup>13</sup> in overpayments in FY 2012-13, which was 0.6% of program expenses.

There are other examples that can be drawn from provincial and territorial governments:

- In 2009, the Auditor General of Ontario reported that Ontario Works overpayments were estimated at \$600 M<sup>14</sup>, partially due to insufficient identity management
- In 2011, British Columbia reported \$260 M in health care fraud, much of which was due to the use of fraudulent CareCards to access services<sup>15</sup>.

It is also difficult to ascertain how much of these overpayments are specifically due to a lack of up-to-date identity information. Some of these amounts may be due to false eligibility information, such as incorrect number of hours worked for EI. However, even if only 10% is due to identity misinformation, Canada's governments have the opportunity to save a considerable sum. Without the ability to definitively determine overpayments due to identity, only illustrative estimates can be used. However, even conservative estimates highlight the need for this initiative. **10% of the examples above still represent \$154M in preventable losses annually to Canada's governments.**<sup>16</sup>

### 1.5.3. SERVICE IMPROVEMENTS

#### BUNDLING

Service bundles are one way to offer an integrated approach to citizens from different organizations to facilitate interactions with multiple service providers across jurisdictions during a single encounter with government. For example, the Newborn Registration Service allows parents to apply all at once for their child's provincial health card, birth certificate, SIN and Canada Child Tax Benefits during the provincial birth registration process. Another popular

12 <http://news.nationalpost.com/news/canada/canadian-politics/ottawa-overpays-ei-by-at-least-300-million-a-year-auditor-general>

13 <http://www.veterans.gc.ca/eng/about-us/reports/departmental-audit-evaluation/2014-audit-of-overpayments/1-0>

14 <http://www.auditor.on.ca/en/content/annualreports/arreports/en11/411en11.pdf>

15 [http://www.canada.com/story\\_print.html?id=88ba8b6f-855b-48b9-8aa5-e9a8204e2700&sponsor=](http://www.canada.com/story_print.html?id=88ba8b6f-855b-48b9-8aa5-e9a8204e2700&sponsor=)

16 Not including municipal benefits programs

example within one level of government is when an individual can automatically send personal information (e.g. name, address and date of birth information) on their tax return to Elections Canada to update the National Register of Electors. Service bundling is already underway in an FPT context as well.

In this context, CDI will allow FPT governments to create new bundles to simplify the interactions with citizens. CDI would allow new service bundles that will simplify citizen interaction with the government, which would lessen the administrative burden on citizens to report changes in circumstances.

## **ONE-STOP**

The concept of a one-stop shop is not new to the online world. CDI will allow more services to work as they are intended: to streamline the application processes. For example, CRA and CBSA are interested in retrieving citizenship and residency data from IRCC to determine eligibility for CRA benefits and control border access, without the need of sending in additional information outside of the initial application. All departments wish to validate identity online, which removes burden from front-line staff and makes a citizen's online interaction faster and easier.

## **PREDICTIVE SERVICES**

CDI's notification feature, as an enabler of digital service offerings, could be leveraged to facilitate predictive services that anticipate life events and proactively offer citizens services based on those events. The Province of Québec already offers services in this manner.

## **2. BUSINESS NEEDS**

Business needs are set goals and objectives for a service. These needs can then be used to inform changes needed to a service. For example, CDI can help enable improvements to a service. The gathered Business Needs intelligence is meant to help clarify the business drivers that will support the need for a pan-Canadian interchange on identity. It also highlights considerations regarding what provincial and federal partners are looking to receive from each other as well as from other jurisdictions in support of their respective business lines.

Given that the scope of the CDI project is identity information, it should be noted that identity information can encompass a number of data elements within the personal information sphere.

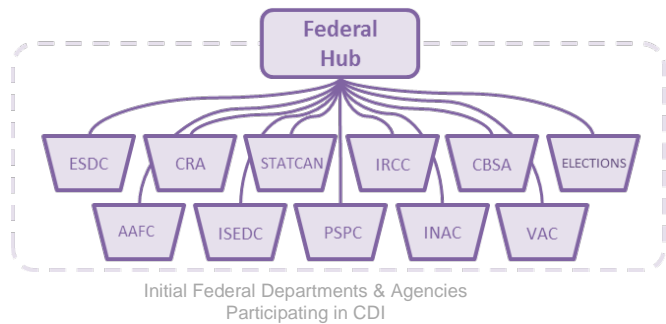
## **AUTHORITATIVE SOURCES**

Stakeholders at both the federal and PT level have identified authoritative data source in each other's jurisdiction as well as their own. Authoritative sources include the basic records that describe identity attributes such as birth, death, address or a person's citizenship status and ability to work in Canada. Six principal authoritative sources were identified as key data sources that would be used as evidence to support the existence of an individual or provide evidence that links an individual to a proven identity by federal departments:

- **Citizenship & Immigration Data (IRCC):** This data allows a relying party to validate identity for individuals who were born abroad but who have been granted citizenship or may have legitimate status in Canada.
- **Social Insurance Register (ESDC):** While Social Insurance Numbers (SIN) are not considered an ID card, SINS are used by many relying parties as a primary identifier. ESDC is the authoritative source for all date of death notifications for SIN enabled programs in the GC.
- **Indian Card Register (INAC):** Allows a relying party to validate the name of every person in Canada who is registered as an Indian under the *Indian Act*.
- **Business Number Database (CRA):** Canada Revenue Agency is an authoritative source for the issuance of the business number only. They are also a trusted source of the business identification information. Note that Québec also offers the Québec Enterprise Number (NEQ) for businesses.
- **PT VSOs:** VSOs can provide relying parties (according to laws and regulations in place) with access to registered vital events data (birth, death, marriage, stillbirth and change of name/sex).
- **PT Transport Ministries & Health Service Ministries:** These organizations provide access to documents that can provide evidence that links an individual claiming an identity to actual identity itself. These sources allow relying parties to match a name, date of birth, and address to the individual who is claiming this identity.

## 2.1. FEDERAL BUSINESS NEEDS

Since 2013, the CDI Federal Operations Committee has been meeting on a regular basis to discuss the development of CDI. The eleven participating members of the Committee contributed to a business needs determination exercise which was conducted from November 2015 to January 2016.



Departments and agencies were asked to identify business lines and programs as well as the authoritative information that each of their respective program could provide to relying parties through a real-time electronic service.

Given that CDI is meant to allow partners to send electronic messages to each other to validate that the identity information of an individual is accurate, it is important to note that the federal needs should be considered partial without the finalization of the PT business needs.

The exercise brought to light a number of general observations that can serve as key drivers for CDI moving forward:

- **Supporting Program Integrity** - Departments and agencies dealing with citizen services primarily rely on the security of their systems and processes for delivering services. To provide a benefit or service, delivery agents all require varying degrees of assurance to know that an individual is who he/she says they are. A number of GC service offerings rely on their internal departmental ecosystem to support program or service integrity as they relate to identity. *CDI is seen as an enabler to facilitate the expansion of authoritative data sources to authenticate program information against someone else's data for the purpose of service delivery.*
- **Supporting Evidence of Identity** – There is a general consensus that “foundational documents” issued by VSOs for individuals born in Canada (birth certificates) and documents issued by IRCC for individuals who were born abroad but have been granted citizenship (Certificate of Canadian Citizenship) or who have a legitimate status in Canada (e.g.: permanent residence, work permit, study permit) serve as key proof that the identity claimed by an individual is legitimate and valid. Expanding access to this information to more partners among all levels of government in a real-time setting will improve efficiencies and transparency while enabling involved stakeholders to potentially reduce identity and benefit fraud. *A number of federal departments and agencies expressed interest in validating identity against additional supporting evidence (e.g. federal and/or PT authoritative sources) in order to increase the confidence level behind their online customer service channel without the need of in-person or out-of-band processes.*
- **Adherence to the GC's Identity Management Policy** - A number of respondents linked their program need responses to ongoing efforts in adhering to the *Identity Management*

*Policy*<sup>17</sup>. In this context, CDI has the potential to enhance data integrity, reduce costs, eliminate inefficiencies as well as lower risk for error as GC stakeholders work to *improve how departments authenticate and provide the legitimacy of an identity claimed by citizens*.

- **Common Data Exchange Standards** - Stakeholders referenced a number of pre-existing ad-hoc connections between departments and agencies and others reinforced the need to expand such connections to simplify or accelerate processes. Data exchange methods currently in place seemed to vary greatly between organizations and programs. Three departments (ESDC, CRA and Statistics Canada) are currently exchanging birth and death information with 10 Provinces using a common data exchange standard (NRS). It is likely that there will be a *need to have a common standard in order for CDI to be an effective solution*. It would improve upon the NRS. The Pan-Canadian Identity Validation Standard has been endorsed by the FPT DM Table on Service Delivery Collaboration. The Pan-Canadian Identity Information Exchange Specification has been drafted and endorsed by the Identity Management Sub-Committee (IMSC).

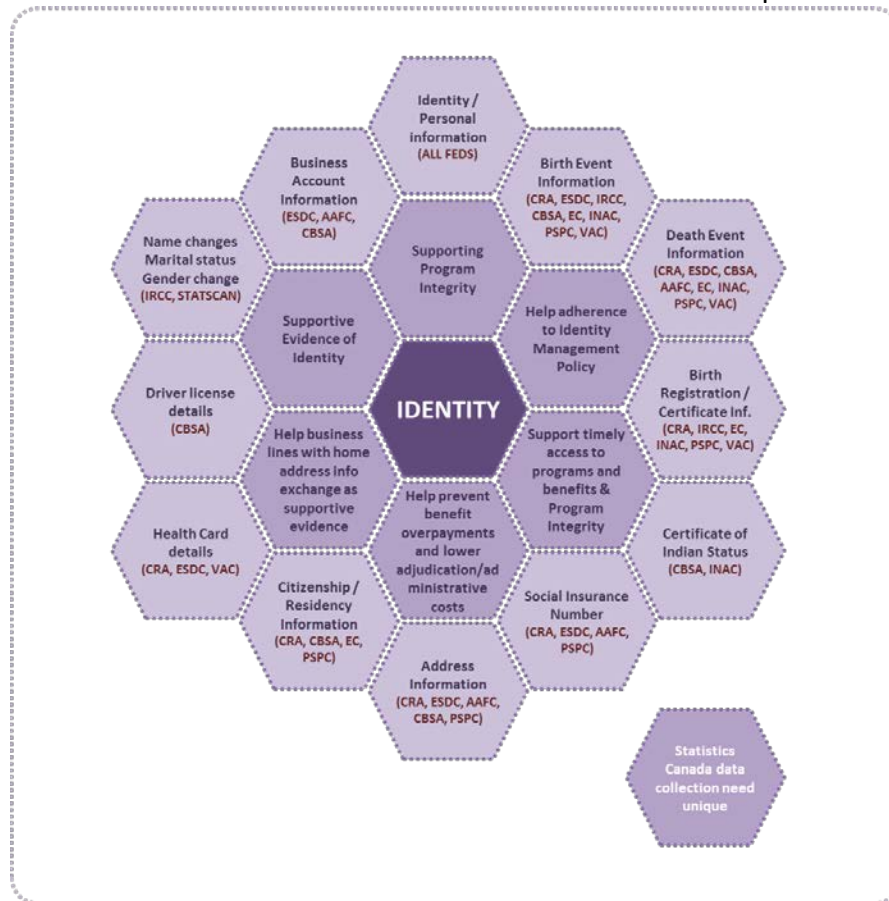
## FEDERAL IDENTITY MANAGEMENT NEEDS

What follows is the collected federal input from departments and agencies synthesized and grouped by need category. The overview is accompanied by summary tables (Annex B) illustrating the need type breakdown for each departments and how they support identity management in the delivery of programs and services. The following diagram summarizes the

---

<sup>17</sup> Identity Management Policy - Treasury Board of Canada - <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577>

identity attributes that were identified in the federal business needs questionnaire exercise.





### 2.1.1. NOTIFICATIONS, VALIDATION AND RETRIEVAL DATA NEEDS

All GC services, both online and in person, require a validation method for an individual's identity to allow citizens to enroll in a service. For departments and agencies, CDI is seen as a unique opportunity to facilitate the upkeep of individual account information for the purpose of direct (real-time) and indirect citizen service interactions.

#### Notification of a Birth or Death Event

Ten of the eleven consulted departments and agencies identified a need to receive birth or death information from VSOs in order to support programs and citizen service delivery agents.

- **Access to Programs and Benefits** - Birth and death notifications were flagged by a number of stakeholders as important information to ensure a citizen or a next of kin is directed to the appropriate program or benefits, thus ensuring that individual data is up to date and citizen eligibility and direct access is triggered following a life event.
- **Timely Notices** - Timely life event notifications were identified as key in preventing benefit overpayments and reducing administrative costs associated with debt-recovery activities.
- **Citizen Data Upkeep** – A number of stakeholders identified the need to be notified automatically when a citizen changes a key data attribute with another partner (e.g. address change, etc.). This was seen as a way to lessen administrative burden and lower risk of fraud and adjudication efforts.

#### Validation and Retrieval of data against PT Organizations

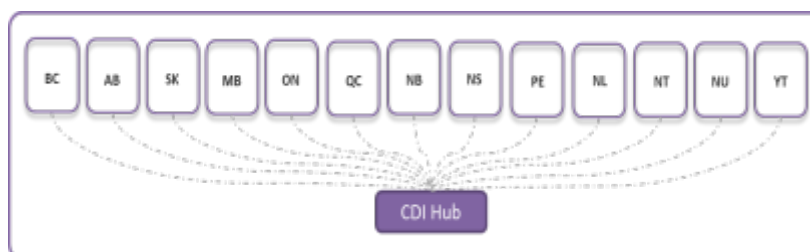
Twenty one programs and initiatives were identified by federal stakeholders. All indicated that they would like to use CDI to support the validation of data function with their programs or services against authoritative sources.

- **Validation through Retrieval to complete Identity Records** - Retrieval is a form of validation where the relying party identifies an individual and asks a question about a citizen to receive supplementary information. Although not directly linked with the identity of an individual, two business lines identified this information exchange transaction type in order to obtain information supplementary data about individuals associated with a Business Number.
- **Mailing Address Information as Supportive Evidence** - Although very few departments or agencies initially recognized the need for the retrieval functionality, a number of stakeholders indicated that an individual's postal address is a key data attribute that programs often have to manage that falls into supportive evidence linking an individual to a proven identity. While no official authority exists for this attribute, stakeholders highlighted some government issued documents such as PT Transport and Health Ministry service cards which have supporting address data that is refreshed on a cyclical basis. CRA's Federal Income Taxes Program or Elections Canada's National Register for Electors were also cited as additional databases that could support be retrieved to support program delivery.

- **Data Collection Need** - Statistics Canada highlighted a unique business need linked with their agency's general data collection/surveying mandate. CDI could support such a need over time through a combination of notifications and retrieval exchanges.

## 2.2. PROVINCIAL AND TERRITORIAL BUSINESS NEEDS

Engagement with various PTs on CDI has been ongoing since 2013. Engagement discussions with provincial and territorial stakeholders on CDI have been conducted through a number of different channels. Formal



Participating CDI Provinces and Territories

engagement on the initiative is received through the Project Oversight and Coordination Committee (POCC), which reports to the Public Sector Service Delivery Council (PSSDC). It has also taken place during identity related fora, through bilateral engagements as well as during discussions with PTs on peer projects such as ILP and the VEL Program (ESDC).

In December 2015, a business needs questionnaire similar to the one sent to CDI Federal Operations Committee members was sent to POCC members to collect formal needs on how each jurisdiction proposes to connect programs, business lines, VSOs and Service Ministries to CDI. PTs were also asked to identify authoritative sources from jurisdictions that would help support them in their service delivery.

PT questionnaire responses are ongoing, the completed responses in conjunction with other engagement activities highlight a number of key considerations to support the development of CDI:

- **Vital Events data** – Information sharing of vital events data is essential (not only with the Government but between PTs) for birth and death notification data. Provinces need this information due to migration from province to province. ESDC currently uses this infrastructure to validate birth information for program delivery.
- **Revenue Generation** – Transaction fees are a key consideration for PTs involved with CDI. PTs currently receive transaction fees from the GC in exchange for birth and death information from VSOs. These transactions account for a portion of the core budget supporting these organizations. Some PTs have recognized that the addition of partners would potentially allow them to increase their revenue generation.
- **Various States of Readiness / PT Data Hubs on Identity** - The state of readiness of PTs varies greatly from one region to the other. Preliminary efforts in coordinating identity data are already in place (e.g. Newfoundland and New Brunswick have established ad-hoc connections to exchange death information between themselves while British Columbia has set up a process to allow any province to access their death information). Some provinces, such as Alberta and Quebec, have already been working on hub technology to connect their internal stakeholders. Alternatively, Ontario has indicated

that they are not considering building a hub, and as a result, the Ontario VSO and service ministries would likely connect directly to a CDI hub to exchange information. Other jurisdictions have recognized that a regional hub may be the most efficient way to move forward (Atlantic Provinces and the Territories).

### 2.2.1. PT IDENTITY NEEDS

Needs to support PT stakeholders are being derived from a combination of what the federal partners identified as supportive data that could be shared with PTs as well as intelligence gathered from the interactions with PT service ministries and VSOs. Two primary requirements have been identified as key element to support existing governmental programs across the country:

#### Access to Identity Data

- **ILP & IRCC Data** – The ILP business case, which is a pathfinder to CDI, has clearly identified that PTs would gain significant benefits from a direct connection to IRCC immigration data. A connection to this data would 1) improve program and data integrity, 2) reduce the risk of fraud to individuals and 3) improve service delivery to Canadians.
- **Fraud Prevention and Program Integrity** - Given that program recipients are often from other jurisdictions, PTs service delivery can greatly benefit from access to life event data from other jurisdictions.
- **Other Possible Federal Authoritative Sources** – With the expansion of federal partners, there is a possibility that PT ministries may wish to gain access to new CDI data sources (e.g. SIR). Further engagement is required to confirm this assumption with each stakeholder. Revenue Québec already has a connection to the SIR.

#### Exchange of Death Events between PTs

- **PT to PT Data Exchange** – CDI will need to enable PT to PT information sharing. Labour mobility has constant impact on programs and services delivery. A successful CDI would allow PTs to access death information in a more rapid fashion.

## 3. FEDERAL INFORMATION SHARING AUTHORITIES & PRIVACY

While many federal departments already have the necessary authority to collect and disclose personal information for the purposes of CDI, some authorities will need to be better defined in legislation or would benefit from additional clarity to reduce risk and increase transparency and efficiency. Information sharing authorities are defined as the permissions contained within legislation for federal departments and agencies to collect and disclose personal information, and to disclose personal information specifically in an electronic format.

Many federal departments and agencies already collect, use and disclose the personal information that would be shared under CDI, through a variety of processes. These departments, ministries or programs have appropriate authorities and information sharing agreements in place for these processes but initiatives such as CDI challenge the current structures and authorities to adapt to the reality of modern service delivery. See Annex C for current federal authorities.

Many departments rely on section 8(2)(a) of the *Privacy Act* to disclose personal information, in conjunction with departmental specific legislation. This section allows departments to disclose personal information when it is consistent with the purposes for which it was collected, as it outlined in the statutory departmental legislation. This section does not restrict the disclosure only to certain entities (e.g., federal government departments and agencies, or PT governments) and therefore, may be sufficient to permit disclosures in all possible scenarios of service providers (e.g. external, third party provider). At this time, use of this provision is subject to interpretation and departmental legal services units have not yet agreed on whether this authority is sufficient.

In addition, some departmental legislation (e.g. *Citizenship and Immigration Act*) currently allows for information to be collected, used and disclosed but the wording often limits such activities to physical documents and requires citizens to “present, provide or show” documents, which implies being physically present. In an electronic service world, this language would need to be clarified to allow for information to be disclosed electronically.

To address gaps, there are several options that could be undertaken to provide participating federal departments and agencies with the necessary information sharing authorities to participate in CDI.

### 3.1.1. BROAD APPROACHES

Authorities for confirming an individual’s identity can be either within existing legislation (e.g., *Privacy Act* or *Personal Information Protection and Electronic Documents Act*) or in a new, standalone piece of legislation. This approach would still require consequential amendments to departmental legislation, including the *Department of Employment and Social Development Act* (DESDA). Analysis has been undertaken and has concluded that taking a broad approach is the simplest from an implementation perspective and would allow all departments and agencies that provide public services to validate all of the identity information that it needs as soon as it comes into force. There are three proposed options below to implement a broad approach, however, it should be noted that any sweeping changes to legislation will take time and have implications to implement/roll out of a CDI service.

The federal government is committed to making it easier to access government services online. To support this commitment, TBS has been given the mandate to develop a GC Client-First Service Strategy. Validating identity information through CDI could lead to more timely service delivery and enable seamless service transactions across jurisdictions.

For these broader options, the information sharing agreement (ISA) model would be streamlined by overarching enabling legislation and data attributes to be exchanged clearly defined, which could lead to less misinterpretation of legislation and increased transparency.

### Amendment to the Privacy Act

This option would see an amendment made to the *Privacy Act* to allow for disclosure for the purposes of confirming the identity of an individual. Proactive disclosure (e.g. notification), as well as information collection powers, would still be based in enabling program or departmental legislation. As Part IV of DESDA overrules the *Privacy Act* and any other Act of Parliament, mirroring amendments would need to be included in that legislation as well.

This option would provide for global information sharing authority, ensuring few roadblocks for departments that are far away from using CDI but wish to use it in the future. It is also one of the highest profile options; amendments to the *Privacy Act* are rare and would be heavily scrutinized by the public and media. While this option streamlines authorities to be included in ISAs, it does not expedite them.

The Standing Committee on Access to Information, Privacy and Ethics (ETHI) has placed a review of the *Privacy Act* on its order of business for the 42<sup>nd</sup> Parliament. The outcome of this study, and the government's response, will be important considerations.

### Potential "Digital Service Delivery Act," limited scope

This option is similar to the *Privacy Act* option but is a standalone bill that contains a bundle of consequential amendments to departmental legislation to collect and disclose information for the purposes of the delivery of services. This can be broader than identity information, defined in regulation or Order-in-Council (OIC). This would allow the scope of the bill to incorporate other amendments necessary to implement the government's service agenda as envisioned in the Ministerial mandate letters.

This option could more precisely capture the purpose and scope of the information being shared than the *Privacy Act* option, for example, by including information that is beyond identity, or not personal information at all (e.g. anonymized payment information). It can include provisions on the business number if necessary.

Rather than being framed in the context of privacy and information protection, discussion over this approach would likely be more balanced between privacy and the delivery of public services. Developing a digital service-specific bill would allow the government to conduct more precise consultations with stakeholders.

In terms of information sharing, considering this option would be more defined with purposes identified, it would assume less risk being more transparent.

## Potential “Digital Service Delivery Act,” ambitious scope

This option is similar to the limited scope option but rather than being simply a collection of consequential amendments, it is a standalone bill to provide global authority to departments to collect and disclose information for the purposes of the delivery of services notwithstanding any other Act in Parliament. The departments affected can be listed by OiC or by schedule of the *Financial Administration Act*. As Part IV of DESDA, overrules the *Privacy Act* and any other Act of Parliament, mirroring amendments would need to be included in that legislation as well.

The scope of the total information permitted to be shared in this bill can be defined in regulation or OiC in order to reflect the future needs for information sharing as more services move into the digital space and the trusted digital identity takes shape. As with the limited scope option, this would allow the scope of the bill to incorporate other amendments necessary to implement the government’s service agenda as envisioned in the Ministerial mandate letters.

### 3.1.2. TARGETED APPROACH

If a broad solution is not feasible, participating departments would need to undertake the targeted approach of amending their enabling legislation to be provided with specific authority to share information to confirm the identity of an individual. This option would see amendments made to departmental enabling legislation led by departments on their own timelines. As each department is responsible for their own enabling legislation and timeline; they would most likely bundle these amendments within broader packages made for non-CDI purposes. Some central support would be provided by TBS and the Department of Justice, e.g. policy objectives, drafting instruction best practices.

This approach would ensure that authorities are in place; however, it would need a great deal of oversight to ensure that all departments and agencies that provide services are included. Also, this may require some departments, such as INAC and VAC, to undertake stakeholder consultation requirements to make the necessary legislative changes, leading to potentially lengthy and involved processes. The approach could require several waves of amendments, which may not be politically feasible, unless those pieces of legislation were being amended for unrelated reasons.

The ISA model to support the implementation of a targeted option would be more difficult to execute due to the different timelines of the amendments and departmental processes that are required.

## SUMMARY OF APPROACHES

	Advantages	Disadvantages
<b>Broad Approaches (Recommended approach)</b>	<ul style="list-style-type: none"><li>As CDI evolves, a broad piece of legislation could be more easily amended and have immediate effect</li><li>Single legislative reference would improve clarity and transparency, minimize challenges in</li></ul>	<ul style="list-style-type: none"><li>May encompass larger whole-of-government legislative needs (e.g. not CDI specific), such as linkages to the broader GC Service Strategy</li><li>Significant effort and must align to broader government priorities</li><li>Consequential amendments to certain</li></ul>

	interpretation across multiple legislative references <ul style="list-style-type: none"> <li>• Could include supporting regulations that mitigate administrative burden for privacy frameworks, enable multilateral approaches</li> </ul>	legislation (e.g., DESDA) would still be required
<b>Targeted Approach</b>	<ul style="list-style-type: none"> <li>• Quicker implementation for those few federal departments and agencies that do not have appropriate authorities to share information</li> </ul>	<ul style="list-style-type: none"> <li>• Amendments are point-in-time, does not support scalability of CDI functionalities or data elements</li> <li>• Maintains existing bilateral policy frameworks</li> <li>• Would not mitigate disputes in legal interpretation of authorities</li> </ul>

### 3.1.3. PRIVACY CONSIDERATIONS & ISA FRAMEWORK

Since the inception of benefits, governments have asked Canadians for identity, eligibility and supporting personal information. Canadians understand that governments need to use personal information for the provision of benefits and services.

The information used and disclosed by parties under CDI would only be used for the purposes of identity validation. These uses are those specifically named in the legislation or regulations of jurisdictions. Furthermore, parties would be restricted to disclosing only the information that they have authority to disclose.

This initiative will not result in the creation of a new personal information bank. There will be no central database of identity information created in any federal department or in an FPT space. CDI would be only the gateway that allows messages to pass from federal departments to jurisdictions and vice versa. Metadata or audit logs would likely be required but these would not contain personally identifiable information.

Throughout the development of CDI, there has been a consensus that privacy protections incorporated in this project must be measured against relevant and test privacy principles. CDI will use the 10 privacy principles articulated in PIPEDA. These same principles are reflected in corresponding provincial legislation. These 10 privacy principles will be part of the greater privacy analysis as part of the CDI design process.

Personal information exchanged via CDI would help strengthen privacy practices pertaining to identity information. The preliminary analysis in Annex D assumes certain design decisions and has been included primarily for analysis and development of a privacy design/implementation plan. A more thorough Privacy Impact Assessment (PIA) and Security Assessment and Accreditation will be undertaken before implementation and exchange of personal information once critical design decisions are made. Overall, the most integral privacy principle is that parties can only validate information provided to them by citizens; they cannot validate for interest or to proactively scan for fraud. This will prevent trolling for personal information that an organization would not otherwise be permitted to collect.



## INFORMATION SHARING AGREEMENT FRAMEWORK

There are two options that could be explored, either the common approach of bilateral agreements between partners, or a multilateral approach with a federal multi-departmental ISA.

### Option 1 – Bilateral ISA Framework

The federal government currently has a myriad of ISAs to govern the sharing of information to support verification of identity and eligibility, both between federal organizations, and between federal and PT organizations. A survey of just five federal departments<sup>18</sup> estimates that **over 650 bilateral ISAs** have been signed since 2003, including federal-to-federal and federal-to-PT agreements. This does not include important parties such as INAC, PWGSC or VAC.

This model is inefficient and costly. ISAs may have different terms and expiry dates, and some may be lost to corporate memory due to employee movement. This leads to potential risks if bilateral agreements are not being honoured or if an organization cannot properly account for information it sends or receives.

ISAs require human resources to maintain and renegotiate, however it is difficult to determine the exact cost of negotiating an identity ISA in particular. As these ISAs are integrated into program delivery, negotiation and implementation costs are subsumed under overall program costs in departments' Program Activity Architecture. One consequence of identity validation being decentralized into programs is the inability for costs to be precisely identified.

An informal survey of departments determined that it took, on average, four FTEs approximately one year to negotiate an ISA, whether between federal departments or between federal and PT entities. Overall estimated costs of negotiating an ISA ranged within \$150K to \$250K per department.<sup>19</sup>

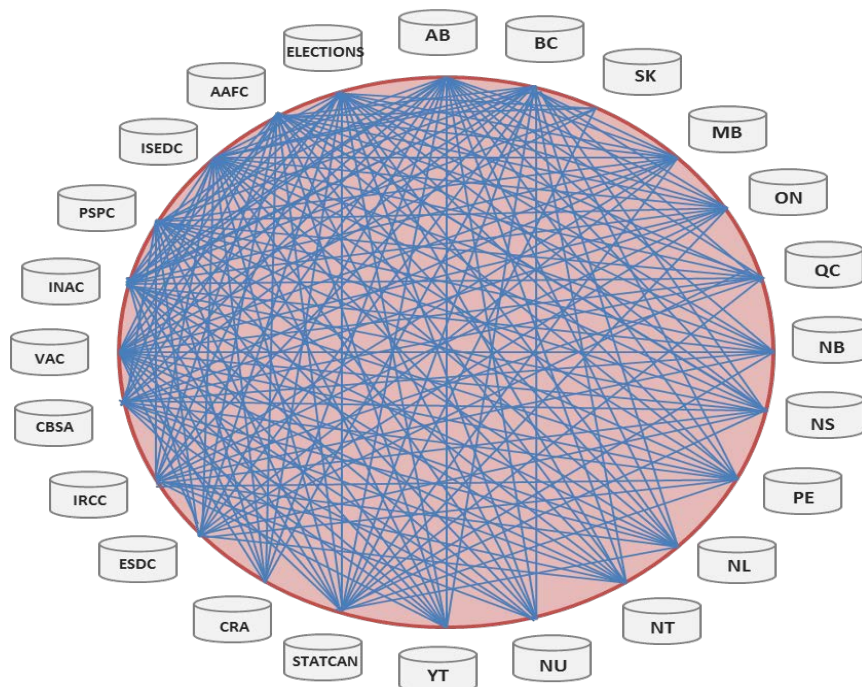
This bilateral CDI model represents a maximum possibility of 1,017 ISAs (120 Fed to Fed, 468 PT to PT, and 429 Fed to PT).

---

<sup>18</sup> CBSA, IRCC, CRA, ESDC/Service Canada, Statistics Canada

<sup>19</sup> Including salary, O&M, legal services and IT expertise

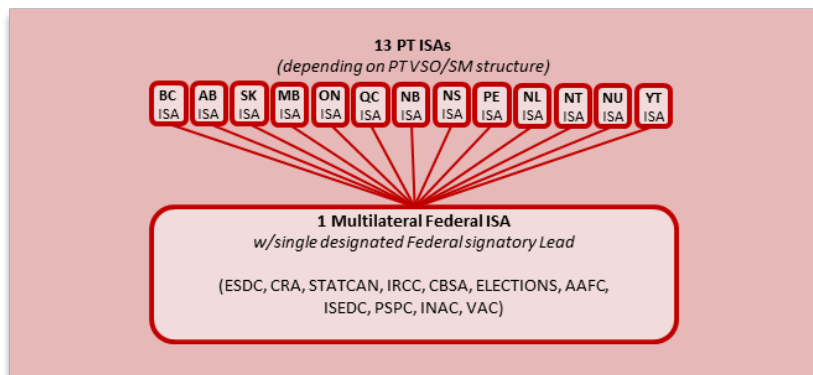




## Option 2 – Federal Multi-Departmental ISA

Currently amongst federal departments and PTs, information sharing agreements are usually bilateral and vary by jurisdiction. Federal departments follow the TB directive on what privacy components need to be included in an ISA; however, there is no common look and feel within the federal family. To alleviate inconsistencies and support strengthening privacy practices, CDI is pursuing the development of a multi-federal ISA framework amongst federal partners that would include a federal designated representative to sign agreements with PT partners (1 federal ISA and 13 PT ISAs).

From a privacy perspective, this ISA framework standardizes privacy provisions while striking the right balance regarding flexibility so new parties can accede to the agreement after it comes into force and any specific information sharing requirements can be added to ensure a **multi-departmental**



(Federal Multi-Departmental ISA, with supporting PT bilateral ISAs)

**ISA framework.** This approach with limited ISAs would eventually replace bilateral agreements that currently exist among and within jurisdictions enabling better protection of personal information and clearer accountability. This ISA framework and supporting PIAs will clearly

outline the parameters around the collection, use and disclosure of personal information (data attributes) identified as part of the CDI service.

By streamlining the ISAs, all CDI parties will be held to the same standards around the following:

- Governance and authorities
- Information management and security
- Access, confidentiality, use, disclosure, retention and destruction of personal information collected under CDI
- Information management and audit
- IT Security and Problem management

FPT partners would be held to the same privacy standards resulting in stronger protection of the personal information provided by Canadians for validating identity. It is envisaged that the FPT governance model chosen would provide guidance on the multilateral ISA framework via a working group.

While there are benefits to a multilateral ISA approach, challenges also remain. There are currently no models to learn from as this approach remains largely untested due to the complexity of so many signatories. This model could also be lengthy at the development stage; however, would be more manageable and less resource-intensive in the longer term regarding amendments and expanding the data elements for exchange.

Once the governance and authorities to support CDI are confirmed, a mandate to negotiate the ISA framework further with partners will be required.

*NOTE: Independent of the authorities chosen to implement CDI or the ISA framework, federal departments will be responsible for respective PIAs, Privacy Notice Statements, Personal Information Banks, and the creation or updating of internal policies associated with CDI.*

#### **4. GOVERNANCE - A PAN-CANADIAN APPROACH**

For CDI to be successful, a pan-Canadian approach is needed – not only with respect to the technological architecture but with a recognition that all jurisdictions have to contribute to the overall strategic direction of the CDI service and to recognize that there is a common concern of identity validation across Canada. Other jurisdictions have taken similar approaches, see Annex E for examples.

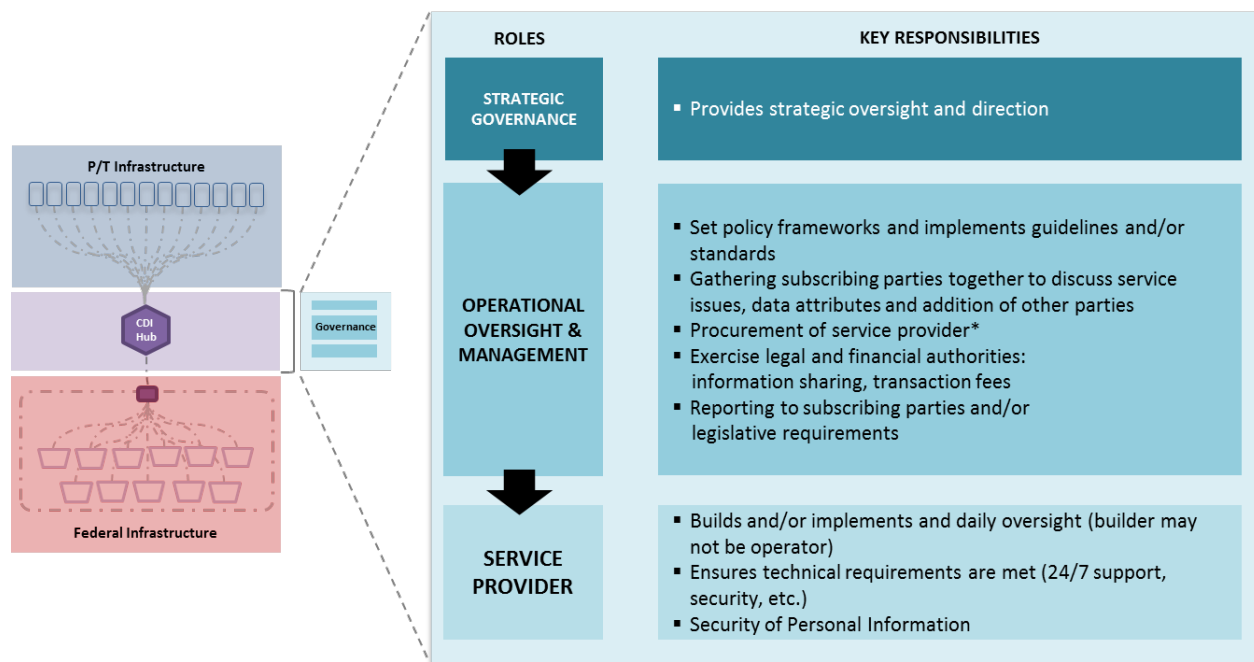
A pan-Canadian governance model should include a strong approach to defining a structure where all participants are represented and can be held accountable for the funding, delivery and operation of CDI. For example:

- Should have a coordinated and connected oversight capability;
- All subscribing parties should have influence on solution decisions and data management, all within approved standards for interoperability, functional services and data;

- Be able to address the complex coordination of the federal, provincial and territorial (PT) governments;
- Be scalable to allow new subscribing parties and lines of business.
- 

The following graphic depicts the proposed governance model and responsibilities for CDI, followed by suggested options for operational oversight body and service provider.

### PROPOSED GOVERNANCE MODEL



#### 4.1. OPERATIONAL OVERSIGHT AND MANAGEMENT

Regardless of the option selected, a FPT entity will be a key player in **providing strategic alignment and priority setting for the overall CDI initiative.**

For example, the FPT Deputy Minister Table on Service Delivery with the support of the Joint Councils articulates a Canada-wide service-delivery vision, taking into consideration the specific context of jurisdictions, priority areas for collaboration, promotes inter-jurisdictional dialogue and co-operation on service delivery issues and provides a forum to establish and meet common goals.

The expertise and knowledge of this membership could provide the strategic oversight function for CDI and ensure the appropriate alignment to the Pan-Canadian Trust Framework and Pan-Canadian Identity Standard. While the FPT entity may be consulted on occasion, the day-to-day management and operational oversight will need to be undertaken by a representative body of participating jurisdictions, including a dedicated GC representative or co-chair. Given that this body would be the effective owner of CDI, it would require dedicated secretariat support.

There are two options to be considered in naming an operational oversight body for CDI: the creation of a FPT shared governance corporation (e.g. not for profit corporation) or decision making through a single FPT Framework Agreement.

### Option 1: Shared Governance Corporation

FPT governments would create a corporation that would be responsible for operational oversight for CDI services on behalf of all jurisdictions. In this option, a board of directors consists of senior executives of FPT service organizations and would set strategic direction. The board would be supported by an Executive Director and a small team of dedicated staff, and would be responsible to appoint officers, employees and agents to carry out day-to-day management activities.

The establishment of a corporation would be reflective of the scale and scope of the operations that would be required, and would also be able to be expanded as CDI grows in scale. There are varieties of types or models of corporations that could be established to execute these functions. For example, a shared governance corporation could be established under the *Canada Non-Profit Corporations Act* that would enable the creation of an independent, shared governance corporation with little reporting requirements that could have scalable membership over time. Instead of creating a new corporation, FPT governments could agree to nominate or transform an existing corporation, to perform these tasks. Similar to a not-for-profit corporation is the development of a *joint enterprise* that would establish corporate entities under varied enabling legislations (e.g., *Corporations Act*) whose shares are partially owned by the federal government with the balance of shares owned by other governments. There are few examples of joint enterprises in Canada at the federal level, and are linked to economic development projects (e.g., Lower Churchill Development Corporation Limited, North Portage Development Corporation).

Within the federal context, the Canadian Council of Motor Transport Administrators (CCMTA) is an incorporated non-profit organization that coordinates all matters dealing with the administration, regulation and control of motor vehicle transportation and highway safety. CCMTA provides collaborative leadership in addressing Canadian road safety priorities through the work of its Board of Directors, including representation from provincial and territorial governments as well as the federal government of Canada (Transport Canada). To support its members, the CCMTA operates a non-intelligent hub to share information between jurisdictions related to the driver records that are issued in other jurisdictions.

A few other examples for these options are the Canadian Blood Services and the Canadian Institute for Health Information (CIHI). CIHI is an independent, not-for-profit organization that provides essential information on Canada's health system and the health of Canadians. They have a 16-member Board of Directors that links federal, provincial, and territorial governments with non-governmental health groups. Other partners included Ministries of health as well as Statistics Canada and Health Canada.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>✓ Legal status independent from Board of Directors and/or membership</li> <li>✓ Can enter into legal contracts and have independent financial holdings</li> <li>✓ Can add partners as CDI evolves</li> <li>✓ Can be enabled by legislation</li> <li>✓ Dedicated executive director and secretariat support</li> <li>✓ Possibility for revenue generation or cost recovery</li> </ul>	<ul style="list-style-type: none"> <li>✗ Regulations and reporting requirements are set by legislation and can include certain restrictions (e.g., bylaws may be subject to public consultation or Ministerial approvals)</li> <li>✗ Less flexible if crown corporation or federal department is chosen for service provider</li> </ul>

## Option 2: FPT Framework Agreement

Under this option, participating jurisdictions would sign on to a formal framework agreement enabling FPT collaboration based on guiding principles and shared priorities and allowing for consensus-based decision making. It is expected that a federal host department or agency would be designated to coordinate this process. Secretariat support would consist of dedicated resources within that federal host department or agency, and would also have a co-host provincial or territorial member that would rotate at regular intervals (e.g. biennially) between member jurisdictions. The secretariat would be established and maintained through dedicated funds (co-managed between federal and P/T governments) and in kind contributions. A good example of this model is the Labour Market Information Council that was established in 2015 under the Forum of Labour Market Ministers.

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>✓ Quicker to implement</li> <li>✓ Flexible enough if crown corporation is chosen as service provider</li> </ul>	<ul style="list-style-type: none"> <li>✗ Will not extend to private sector easily</li> <li>✗ Competing membership interests</li> <li>✗ Capacity issues (slower to react to timely issues)</li> </ul>

## 4.2. SERVICE PROVIDER OPTIONS

The second level of the governance structure is more operational. This level includes the critical policies and procedures agreed to by all parties during uncommon events. This service provider would be responsible for the building, implementation and operational requirements for the CDI service.

The rated criteria that could be used for assessing viable service provider options to be the operator reporting to the decision making body are the following:

## Rated Criteria

- **Cost:** A pan-Canadian CDI service would have costs associated with it, such as infrastructure, maintenance, and ongoing administration, possibly consisting of both personnel and assets. The preferred service delivery provider would provide a reasonable cost to deliver the CDI service (including both the build and on-going delivery of the CDI service).
- **Scalability:** CDI will begin by offering validation, notification and retrieval services for subscribed and approved relying parties. These are limited services that respond to business needs of today; however, any service delivery provider will need to be able to expand wider (e.g. be able to carry more types of information, for more partners) and/or deeper (e.g. be able to carry a broader suite of identity services as per the Pan-Canadian Identity Trust Framework). One way or another, CDI will be a small but vital element in a broader, emerging digital identity ecosystem that is being co-created by the public and private sectors through the IMSC and the Digital Identity and Authentication Council of Canada. Ideally any service provider chosen could expand the services it offers to individuals, the private sector and governments promptly (e.g. verifying identity for the issuance of a trusted digital ID, ID repair or reclamation services, cross-sectoral change of address services, etc.).
- **Complexity of Implementation:** Service providers will be able to respond to the development specifications for CDI at different speeds. The options presented will have to include some estimate of the length of time for a build and launch phase of CDI based on business and technical requirements. The perception of risk, liability and political buy-in may have an impact on the feasibility and timeliness of certain options.
- **Demonstrated capacity:** Service providers have different business and technical capabilities, and thus different implementation risks. The service provider should have experience in successfully implementing projects similar in size and complexity.

Each of these service provider options would require an examination of authority to build and operate something like CDI, but also to ensure that CDI subscribing parties have the ability to send personal identity information to or through whatever infrastructure is employed.

There are three options to be considered in naming a service provider for CDI: choosing an existing federal department, crown corporation or private managed service.

### Option 1: Existing federal department

In this option, an existing federal department would provide the services needed to run CDI. An example of this option could include SSC, CRA or ESDC. Any federal department taking on this function would be described in legislation through an OiC, if necessary.

- **Cost:** Within federal departments, there is existing A-based and Operations & Maintenance dedicated funding to identity programs and related IT infrastructure. The knowledge and expertise of existing resources could support the development of CDI.

Costs would be incurred to build the service infrastructure, but may be able to leverage existing IT development activities.

- **Scalability:** Existing investments (e.g. ESDC Enterprise Service Bus, GC Interoperability Project) are able to manage the number of transactions required by federal departments; however whether this is extensible to a wider range of identity-related transactions required for CDI service needs to be determined.
- **Complexity of Implementation:** Federally, any department other than PSPC or SSC would require using one of these departments to procure and/or maintain the infrastructure. An additional mandate would need to be obtained via a mix of legislation and OiC, depending on the organization. Currently, ESDC does not have the authority to provide the services described above to PTs for federal or PT purposes. There are several policy considerations that would need to be addressed. Under the regulations that list the federal institutions with which ESDC may share information for outlined purposes given program requirements, would be the subject of those arrangements. Expanding that role would require amendments to the *Privacy Act* and to federal departments which may not be entirely under the control of ESDC. SSC has the authority to provide the services described for federal departments and between federal departments and PTs; and between PTs themselves.
- **Demonstrated Capacity:** SSC has a mandate to provide centralized infrastructure services to the GC, and has implemented and is in the process of implementing some GC-wide projects, but not expressly for pan-Canadian services. In the instance of other existing federal departments or agencies, ESDC only has projects supporting GC-level partners.

## Option 2: Crown Corporation

CDI services would operate as a sector within a Crown corporation which would be responsible for offering all of the CDI services on behalf of all jurisdictions. Crown corporations are public institutions that are unique legal entities, operating at arm's length from government. Crown corporations are often used to advance policy priorities and objectives, and can have varying spheres of influence and asset bases. The structure and financing of Crown corporations allows for autonomy as an arm's length provider of services, where management and oversight risks are generally lower than with a private sector organization.

For example, Canada Post is a Crown corporation that has already introduced a digital identity proofing service that it offers to businesses, using its wide network of service locations to provide in-person verification. After the identity is verified and stored within Canada Post's systems, future validations against it can be offered in real-time, using a transaction fee payment model.

- **Cost:** This option would require a Crown corporation to leverage its own funding from its business revenue to invest further in this area. A Crown corporation could be expected to operate CDI on a for-profit basis, which could mean higher transaction fees.
- **Scalability:** This option affords significant ability to have the CDI service evolve over time. A Crown corporation could potentially bundle other services such as e-billing, secure



information storage and change of address services with the identity and credential based on citizen consent and their existing business lines. **Complexity of Implementation:** This option would require legal due diligence that said services are offered within its current legislated mandate. The only hurdle of significance would then be to receive PT concurrence with the approach, including their legal and technical ability to connect to a Crown corporation. For example, a commercial entity may have difficulty to negotiate the required agreements with PT VSO and other PT agencies; depending on PT legislation, PTs may be prevented from disclosing to the Crown corporation.

- **Demonstrated Capacity:** These criteria would be evaluated upon selection of a Crown corporation.

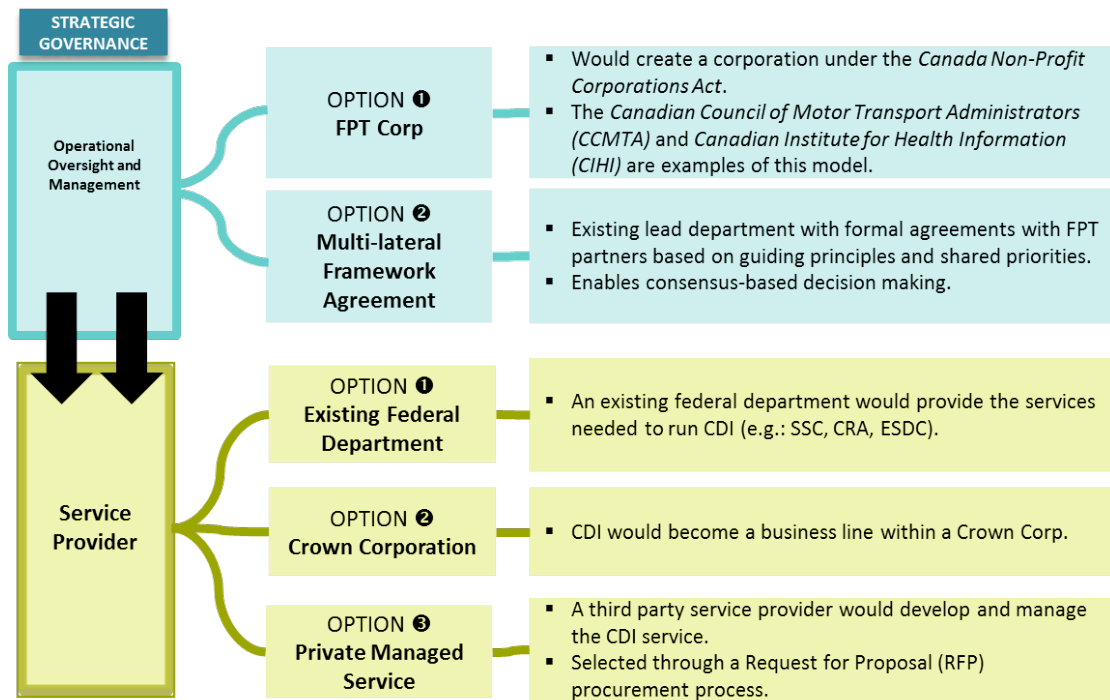
### Option 3: Private managed service

In this option a private, third party service provider would develop and manage the CDI service, would be selected through a Request for Proposal (RFP) procurement process. The system procured would be similar to the public sector hosted solution, in that the technical requirements should be the same.

- **Cost:** Based on a Request for Information (RFI) that was conducted in May 2015, it was determined that preliminary costs for a CDI service would be between \$8-\$14M depending on the service provider and architecture chosen. As preliminary business requirements have been refined, decisions on the architecture and governance are necessary to support a more realistic and rigorous cost assessment in a second RFI and/or RFP process.
- **Scalability:** A RFP would obligate a service provider to match the criteria identified for future scalability.
- **Complexity of Implementation:** It is assumed that a third party service provider would have the flexibility and capacity to develop and build a solution more quickly than the federal government. While the speed of implementation within the government is impacted by departmental capacity, the RFP would stipulate and incentivize timelines for development and delivery.
- **Demonstrated capacity:** Based on the 2015 RFI, there are several private sector organizations that have developed secure messaging services. A second RFI and/or RFP would help identify the demonstrated capability and project experience of the private managed service.



#### 4.3. GOVERNANCE MODEL SUMMARY



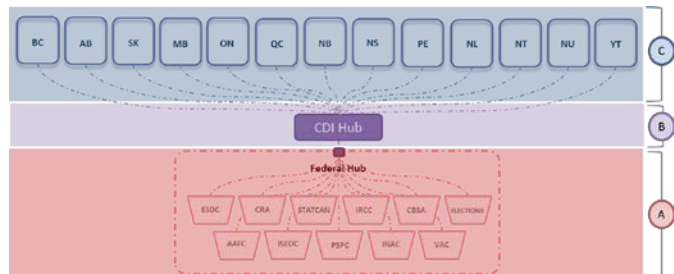
	Existing federal department	Crown Corporation	Private Managed Service
FPT Corporation	Compatible	Least Compatible	Compatible
FPT Framework Agreement	Compatible	Compatible	Compatible

## 5. ANTICIPATED COSTS

### 5.1. TECHNICAL COSTS

In order to build CDI, information will need to be exchanged *between and among GC departments/agencies, and PTs*. This will require a scaled infrastructure build, consisting of three separate components:

- Federal Interoperability Solution (Federal hub)
- Central Infrastructure (CDI Hub)
- PT Infrastructure



The proposed cost analysis focuses on presenting an information exchange solution that meets the identified needs for a central CDI infrastructure. This would be a solution which enables jurisdictions (provincial and federal) to exchange information with each other as well as with other stakeholders. Note that while the needs have been identified, further discussions need to take place to see if needs can be implemented (example: federal departments hope to access driver's license information but this may not be possible).

*Note: PT business needs have yet to be fully determined and further engagement/analysis will be undertaken as CDI moves forward. In addition to PT business needs, there are additional elements such as architecture, governance, information sharing agreements etc. that need to be determined in order to inform, analyze and present the final CDI costing information.*

On both sides of the FPT CDI ecosystem, there will be a need to adapt current IT systems and business processes to allow these to integrate into the CDI ecosystem.

## Federal Interoperability Solution (Federal Hub)

### Federal Infrastructure - Build Costs

This infrastructure will be used to support information exchange between federal departments with a central piece of infrastructure.

ELEMENTS	LOW	HIGH
Hardware	\$1,800,000	\$3,600,000
Platform Build	\$ 410,000	\$ 820,000
Software Licensing	\$1,205,000	\$2,410,000
Solution Design	\$ 200,000	\$ 400,000
Federal Infrastructure Cost (GC internal Network connection costs to a Federal Hub)	\$2,626,000	\$5,252,000
Additional Federal Infrastructure Development Costs (e.g.: modifying departmental systems)	TBD	TBD
Security	TBD	TBD
<b>Total</b>	<b>\$6M</b>	<b>\$12.4M</b>

### Federal Infrastructure - Service Costs

Federal service costs are based on the most common high-level business needs reported by federal partners. Each service that needs to be set up costs \$500,000. These business needs equate to services which take the form of a notification or validation/retrieval of select pieces of information.<sup>20</sup>

It is assumed that each department would have one application/solution that needs to have services added to.



Further costs to connect internal applications have not been included.

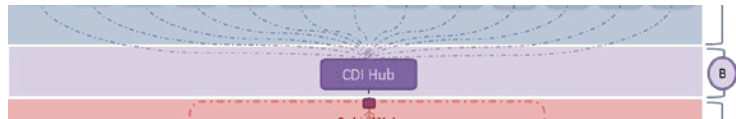
Example: ESDC uses an Enterprise Cyber Authentication Solution (ECAS) for users to register for EI. This same solution is used for OAS and CPP users but the addition of services would only need to be done once on ECAS.

<sup>20</sup> This is based on the development work to set up a service between ESDC's Social Insurance Register and IRCC's Global Case Management System.

Required Services to set up for Authoritative Parties	Cost for Service Development	Cost Model
<b>3 Services</b>	<b>\$1.5M</b>	<b>Based on equivalent ESDC Development work (SIR → GCMS) ~500K per CDI Service</b>
Required Services to set up for Relying Parties	Cost for Service Development	Cost Model
6 Services	\$3M	Based on equivalent ESDC Development work (SIR → GCMS) ~\$500K per Service
<b>Multiplied by 11 Federal Departments</b>	<b>\$33M</b>	

### Central Infrastructure (CDI Hub)

This central infrastructure (CDI Hub) will broker information exchanges between the federal government, PTs, and potentially private organizations.



Costing estimates are based on developing a centralized, pan-Canadian infrastructure and to connect partners to that architecture. PT analysis could yield an alternative architecture solution. For example, the Government of Alberta has indicated that they do not support central hub architecture if they simply want to send/receive information with another province. Alternative models will be analyzed once CDI has a formal mandate to engage partners. Until then, the central CDI hub is the only solution which will be costed at this time.

This estimate includes the central infrastructure build and onboarding costs. There are some unknown cost elements which contribute to the budget range. It was derived from comparable hub infrastructure set up by ESDC's Departmental Service Bus.

A detailed RFI/RFP will need to be completed to obtain updated private sector costs that reflect the chosen architecture. Costs associated with the proposed build:

ELEMENTS	LOW	HIGH
CDI Service Bus		
▪ Hardware	\$1,800,000	\$3,600,000
▪ Platform Build	\$410,000	\$820,000
▪ Software Licensing	\$1,205,000	\$2,410,000
Services Development (17 identified CDI Services)	\$5,900,000	\$11,800,000
Connectivity	\$120,000	\$240,000
Services Implementation	\$10,300,000	\$20,600,000
<b>Total</b>	<b>\$19.7M</b>	<b>\$39.4M</b>

*Note: Operation and maintenance costs have not been included within these figures. Based on comparable projects, there would be an additional cost of 20% added to the figures above to account for these costs.*

## PT Infrastructure

### PT Infrastructure – Build Costs

This proposed CDI infrastructure would allow PTs to exchange information between each other as well as with federal government departments. This would be done through a central infrastructure (the CDI Hub). How PTs decide to implement an information sharing system behind their single connection would be up to them and could vary widely from one province to another. The Québec government mentioned that re-use of the NRS should be considered to reduce costs.



PT engagement is still ongoing. Costs associated with PT infrastructure will be clarified once CDI begins formal negotiations with PT stakeholders.

A rough order of magnitude costing exercise for PT costs has been done using a similar recent ESDC IT projects on interoperability-type infrastructure (e.g. NRS/VEL, SIR-GCMS, Departmental Service Bus, etc.).

### PT Infrastructure - Service Costs

Much like the federal infrastructure service costs, each service that needs to be set up costs \$500,000. This is based on the development work to set up a service between ESDC's SIR and IRCC's GCMS.

It is assumed that each department would have one application/solution that needs to have services added to. Further costs to connect internal applications have not been included.

Required Services to set up for Authoritative Parties	Cost for Service Development	Cost Model
5 Services	\$2.5M	Based on equivalent IT ESDC Development work (SIR → GCMS) \$500K per Service
<b>Multiplied by 13 PTs</b>		<b>\$32.5M</b>

Required Services to set up for Relying Parties	Cost for Service Development	Cost Model
7 Services	\$3.5M	Based on equivalent IT ESDC Development work (SIR → GCMS) ~\$500K per Service
<b>Multiplied by 13 PTs</b>		<b>\$45.5M</b>

ELEMENTS	LOW	HIGH
Additional PT Infrastructure Development costs	TBD	TBD
<b>TOTAL – Technical Costs</b>	<b>\$57.6M</b>	<b>\$114.2M</b>

While costs for relying party information exchange are a valid item for costing, it is believed that these costs will be covered by the respective department or jurisdiction needing that data. As such, they are not included in the final totals.

## 5.2. BUSINESS COSTS

It is important to note that there will be additional effort for a CDI partner to change its processes, policies, procedures, or legislation in order to adopt the use of CDI for any of its functionalities. These are costs outside of the technical costs listed above. As business needs of the PTs continue to be determined and limited knowledge of the current state of both PT and federal departmental IT systems, the following costs have not been included within the estimates:

- Governance costs
- Business process transformation
- Authoritative Party systems development costs
- Relying Party systems development costs
- PT infrastructure costs (including hub)
- Maintenance
- Data center/hosting services
- Migration Costs (NRS to CDI)
- Project Management Costs (approx. 12.5% after total has been established)

### 5.3. PAYBACK

The following is a summary of items identified in the Benefits Realization section on potential savings.

ELEMENTS	POTENTIAL SAVINGS
Elimination of postage – EI Program	\$2M
Reduction of ISA negotiations	\$803K - \$935K <sup>21</sup>
Overpayments	\$155M
<b>TOTAL</b>	<b>\$158M~</b>

### 5.4. COSTING SUMMARY

The costs are estimated in the range of \$57.6M - \$114.2M for CDI at the moment, but this could change significantly due to the number of costs still to be determined listed in the above sections: *Additional Federal and PT Infrastructure Development Costs (e.g.: modifying departmental systems)* and *security* as well as the business costs listed above (section 5.2)

## 6. PATH FORWARD

This business case has been drafted following the direction from DM SFI in August 2015 to further refine the key elements of a possible CDI service. These efforts have been led by federal departments of TBS and ESDC, in collaboration with the CDI Federal Operations Committee and the FPT Project Oversight and Coordination Committee. It is with these partners that this business case has been able to determine the scope of CDI, its value proposition, and business needs, and undertake a more thorough analysis of legislative authorities and present approaches for both public and private sector delivery.

The key conclusions of this exercise have confirmed that there is a need to develop CDI to be a scalable, interoperable solution that provides a secure identity validation service. This service will support the efforts of many jurisdictions in the delivery of digital, on-line services and provide benefit and value to Canadians. To be a truly pan-Canadian service, it must also have shared governance across its FPT partners. The analysis has also highlighted areas where further analysis and/or collaboration with PTs are required in order to make informed decisions around the future design of the CDI service.

It is proposed that the existing governance structure for CDI be leveraged for these engagement activities, with this report and its analysis disseminated to the FPT Deputy Minister Table on Service and the bodies of the Joint Councils (the Public Sector Chief Information Officer Council and the Public Sector Service Delivery Council). The anticipated meeting of the Joint Councils in September 2016 would be an opportunity to share the

---

<sup>21</sup> \$73K-\$85K x 11 Departments

business case, as well as seek a commitment to collaborate on the outstanding design elements that would support the development and launch of a CDI service.

On a parallel track with this engagement, certain elements outlined within this analysis that leads to a series of possible actions that could be taken by the federal government over the short-term to support the future development of a CDI service and to support related priorities such as the development of the GC Service Strategy, such as:

***Authorities to support information sharing:*** To facilitate the sharing of personal information, including identity information, the federal government could begin work on amending existing legislation or the creation “standalone” enabling legislation to support digital service delivery. This could also be achieved by leveraging efforts on the broader GC Service Strategy. In addition, development of a multidepartmental information sharing agreement could begin to support information exchanges between federal departments.

***On the development of federal infrastructure:*** Continued engagement with federal departments and agencies will ensure that the CDI service is designed to meet evolving business needs. Also, there is sufficient need to ensure that within the federal family, identity information is able to be shared, and there needs to be a federal infrastructure to support those exchanges. There is an opportunity to explore if on-going work with the development of the GC Service Bus or interoperability solution could be that federal infrastructure. This would not only demonstrate to provincial and territorial partners that concrete actions are being taken, but would deliver on needs identified by federal departments/agencies.

***Identity Linkages Project (ILP):*** As of June 2016, all 10 provincial visits were completed. ILP is now moving towards the onboarding of the first province by November 2017 with intent of a subsequent provinces onboarding every two months thereafter. Quebec was the first province to confirm interest in two of the three business requirements. A follow up package containing a questionnaire, costing template, transaction fee bands and architectural design was sent out to the provinces in early August to the remaining 9 provinces to seek commitment by the end of September 2016 for onboarding.

***Death Notification:*** With the development of the Death Registration and Notification Blueprint collaboratively with ESDC and the PSSDC, detailed business process maps of the death registration and notification processes by jurisdictions will be analysed to develop a “blueprint” to further improve these processes. This process is a key “use case” for how jurisdictions may be able to leverage CDI to further align identity approaches across jurisdictions and further the development of “Tell Us Once” approaches to service delivery.

With the endorsement of this high-level business case from DM SFI, there is a need to further engage and collaborate with PT partners to validate these findings, further enhance the analysis done to date, and to seek a commitment to move forward with a pan-Canadian governance model. It is through these engagement activities that key design elements can be further refined and agreed to, ensuring that the investments made will be of value and real improvement to existing practices and technologies.



## ANNEX A – GLOSSARY

The definitions that follow include authoritative definitions from the *Standard on Identity and Credential Assurance*, definitions found in related guidelines and industry references, and definitions developed for the Pan-Canadian Identity Validation Standard, which was approved by the FPT DM Table on Service Delivery.

Term	Definition
<b>anonymous credential</b>	Refers to a credential that, while still making an assertion about some property, status, or right of the person, does not reveal the person's identity. A credential may contain identity attributes but still be treated as anonymous if the identity attributes are not recognized or used for identity validation purposes. Anonymous credentials provide persons with a means by which to prove statements about themselves and their relationships with public and private organizations anonymously.
<b>assigned identifier</b>	A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between persons without the use of any other identity attributes.
<b>assurance</b>	A measure of certainty that a statement or fact is true.
<b>assurance level</b>	A level of confidence that may be relied on by others.
<b>assurance of credential</b>	Concerns the binding of a credential to a person (without regard to their identity).
<b>assurance of identity</b>	Concerns the claim that the person is really who they say they are.
<b>attribute</b>	A property or characteristic associated with an entity. See also "identity attribute".
<b>authentication</b>	The process of establishing truth or genuineness to generate an assurance of credential or identity.
<b>authoritative party</b>	A federation member that provides assurances of credential or identity to other federation members (i.e. "relying parties").
<b>authoritative source</b>	A collection or registry of records maintained by an authority that meets established criteria.
<b>biological or behavioral characteristic confirmation</b>	A process that compares biological (anatomical and physiological) characteristics in order to establish a link to a person (e.g. facial photo comparison).
<b>biometrics</b>	A general term used alternatively to describe a characteristic or a process. It can refer to a measurable biological (anatomical and physiological) or behavioural characteristic that can be used for automated recognition. It can also refer to automated methods of recognizing an individual based on

	measurable biological (anatomical and physiological) and behavioural characteristics.
<b>citizen</b>	The intended recipient for a service output. External citizens are generally persons (Canadian citizens, permanent residents, etc.) and businesses (public and private sector organizations). Internal citizens are generally public service employees and contractors.
<b>context</b>	A set of circumstances, a situation, or a scenario in which a person interacts with other persons or with an organization.
<b>credential</b>	A unique physical or electronic object (or identifier) issued to, or associated with, a person, organization, or device (e.g. key, token, document, program identifier).
<b>credential assurance</b>	The assurance that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).
<b>credential assurance level</b>	The level of confidence that a person, organization, or device has maintained control over the credential with which they have been entrusted (e.g. key, token, document, identifier) and that the credential has not been compromised (e.g. tampered with, corrupted, modified).
<b>credential federation</b>	A federation established for the purpose of credential management.
<b>credential risk</b>	The risk that a person, organization, or device has lost control over the credential with which they have been entrusted.
<b>document authentication</b>	The process of confirming the authenticity of a document: genuine, counterfeit, forged, etc. Document authentication is achieved by checking the security features of a document, such as secure laminate, holographic images, etc.
<b>documentary evidence</b>	Any physical record of information that can be used as evidence. This is widely understood to mean information written on paper, but the more general definition is preferable.
<b>documented sex</b>	An attribute copied from the “sex” or “gender” indicator on a credential.
<b>electronic or digital evidence</b>	Any data that is recorded or preserved on any medium in, or by, a computer system or other similar device. Examples include database records, audit logs, and electronic word processing documents.
<b>evidence of identity</b>	A record from an authoritative source that supports the integrity and accuracy of the claims made by a person. There are two categories of evidence of identity: foundational and supporting. See “foundational evidence of identity” and “supporting evidence of

	identity”.
<b>federated credential management</b>	The sharing of assurances of credentials with trusted members of a federation.
<b>federated identity management</b>	The sharing of assurances of identity with trusted members of a federation.
<b>federating credentials</b>	The process of establishing a federation in which members share assurances of credentials with trusted members of the federation.
<b>federating identity</b>	The process of establishing a federation in which members share assurances of identity with trusted members of the federation.
<b>federation</b>	A cooperative agreement between autonomous entities that have agreed to relinquish some of their autonomy in order to work together effectively to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability.
<b>foundation name</b>	The name of a person as indicated on an official record identifying the person (e.g. vital statistics record, immigration record).
<b>foundation registry</b>	A registry that maintains permanent records about persons who were born in Canada, persons who are Canadian but who were born abroad, or persons who are foreign nationals who have applied to enter Canada.
<b>foundational evidence of identity</b>	Evidence of identity that establishes core identity information such as surname, given name(s), date of birth, sex, and place of birth. Examples include records of birth, death, immigration, or citizenship originating from a jurisdictional authority.
<b>gender</b>	The socially constructed roles, behaviours, activities, and attributes that a given society considers appropriate for a male or a female.
<b>identifier</b>	The set of identity attributes used to uniquely distinguish a unique and particular person, organization, or device.
<b>identity</b>	A reference or designation used to distinguish a unique and particular person, organization, or device.
<b>identity assurance</b>	A measure of certainty that a person, organization, or device is who or what it claims to be.
<b>identity assurance level</b>	The level of confidence that a person, organization, or device is who or what it claims to be.
<b>identity attribute</b>	A property or characteristic associated with an identifiable person, organization, or device; also known as an identity data element.

<b>identity claim</b>	An assertion of the truth of something that pertains to a person's identity.
<b>identity data element</b>	See “identity attribute”.
<b>identity establishment</b>	The creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs, and services.
<b>identity federation</b>	A federation established for the purpose of identity management.
<b>identity fraud</b>	The deceptive use of personal information in connection with frauds such as the misuse of debit/credit cards or applying for loans using stolen personal information.
<b>identity information</b>	The set of identity attributes that is sufficient to distinguish one person from all other persons within a program/service population and that is sufficient to describe the person as required by the program or service. Identity information is a subset of personal information.
<b>identity information notification (or “notification”)</b>	The disclosure of identity information about a person by an authoritative party to a relying party that is triggered by the establishment of the person’s identity, a change in their identity information, or an indication that their identity information has been exposed to a risk factor (e.g. the death of the person, use of expired documents, a privacy breach, fraudulent use of the identity information).
<b>identity information retrieval (or “retrieval”)</b>	The disclosure of identity information about a person by an authoritative party to a relying party that is triggered by a request from the relying party.
<b>identity information validation (or “validation”)</b>	The confirmation of the accuracy of identity information about a person as established by an authoritative party. Note: Identity information validation does not ensure that the person is using their own identity information, only that the identity information the person is using is accurate and up to date.
<b>identity management</b>	The set of principles, practices, processes, and procedures used to realize an organization's mandate and its objectives related to identity.
<b>identity resolution</b>	The establishment of the uniqueness of a person within a program/service population through the use of identity information.
<b>identity risk</b>	The risk that a person, organization, or device is not who or what it claims to be.
<b>identity theft</b>	The preparatory stage of acquiring and collecting someone else's personal information for criminal purposes.
<b>identity verification</b>	The confirmation that the identity information being presented relates to the person who is making the claim.

<b>interoperability</b>	The ability of organizations to operate synergistically through consistent security and identity management practices.
<b>jurisdictional hub</b>	A system that all entities within a jurisdiction connect to in order for them to electronically interact with all other jurisdictions via one external facing common gateway.
<b>knowledge-based confirmation</b>	A process that compares personal or private information (i.e. shared secrets) to establish a person's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information, and credit or financial information.
<b>legal presence</b>	Lawful entitlement to be or reside in Canada.
<b>person</b>	A human being including “minors” and others who might not be deemed to be persons under the law.
<b>personal information</b>	Information about an identifiable person.
<b>personal information notification</b>	The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by the establishment of the person’s identity or a change in their personal information.
<b>personal information retrieval</b>	The disclosure of personal information about a person by an authoritative party to a relying party that is triggered by a request from the relying party.
<b>personal information validation</b>	The confirmation of the accuracy of personal information about a person as established by an authoritative party.
<b>physical possession confirmation</b>	A process that requires physical possession or presentation of evidence to establish a person's identity.
<b>preferred name</b>	The name by which a person prefers to be informally addressed.
<b>primary name</b>	The name that a person uses for formal and legal purposes.
<b>relying party</b>	A federation member who relies on assurances of credential or identity from other federation members (i.e. “authoritative parties”).
<b>risk</b>	The uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.
<b>sex</b>	The biological characteristics that define a human being as female or male. These sets of biological characteristics are not mutually exclusive as there are persons who possess both female and male characteristics.
<b>supporting evidence of identity</b>	Evidence of identity that corroborates the foundational evidence of

	identity and assists in linking the identity information to a person. It may also provide additional information such as a photo, signature, or address. Examples include social insurance records; records of entitlement to travel, drive, or obtain health insurance; and records of marriage, name change, or death originating from a jurisdictional authority.
<b>trust</b>	A firm belief in the reliability or truth of a person or thing.
<b>trust framework</b>	A formalized scheme that ensures that federation members have continued confidence in one another. A trust framework formally underpins trust relationships by stipulating adherence to standards, formalizing assessment processes, and defining roles and responsibilities of multi-party arrangements.
<b>trust relationship</b>	A defined arrangement or agreement that ensures confidence.
<b>trusted referee confirmation</b>	A process that relies on a trusted referee to establish a link to a person. The trusted referee is determined by program-specific criteria. Examples of trusted referees include guarantors, notaries, and certified agents.

## ANNEX B – FEDERAL BUSINESS NEEDS SUMMARIES

Business Line Name

### CRA Individual Identification System (Ident)

Department/Agency

Canada Revenue Agency (CRA)

#### Service Offering

The CRA Individual Identification (Ident) system is the Agency's centralized system for all individual identity information accessed and utilized for all programs that serve individual taxpayers and benefit recipients.

Connecting to CDI would enable the CRA to continue to create identity records for individual taxpayers and determine individual eligibility for a variety of benefit programs. Overall, that CDI link with other F/P-T stakeholders would assist the CRA, when necessary, in authenticating an individual's identity when creating/registering to online services.

#### Functionality Type

##### 1 Validation

- Validate the Health Card/Driver's License with PT SM and a Canadian Passport as a secondary source of validation to meet a higher Evidence of Identity Standard when authenticating an individual prior to granting online CRA access.

~24M/yr

##### 2 Notification

- Receive Notifications of birth
- Receive Notifications of death
- Receive change of address from P-T VSO/SM
- Receive SIR info from ESDC
- Send address change information to Elections Canada.

~24M/yr

##### 3 Retrieval

- Retrieve citizenship/residency info for Benefits recipients from IRCC

~24M/yr

#### Data Attributes

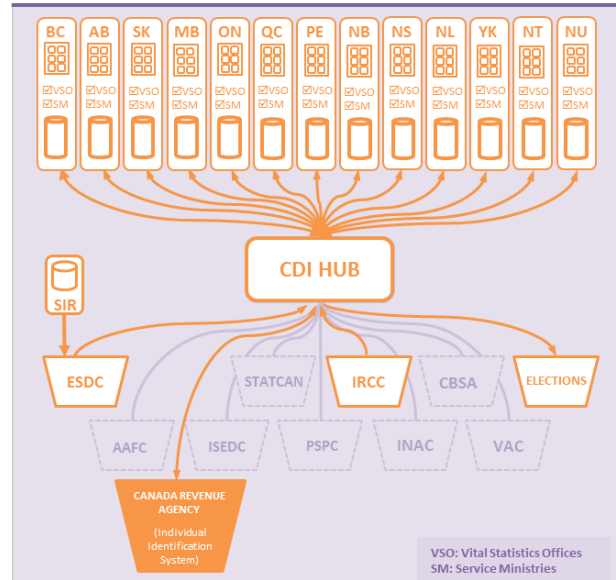
- First Name (ESDC-SIN-EP)
- Surname (ESDC-SIN-EP)
- Gender (ESDC-SIN-EP)
- Date of Birth (ESDC-SIN-EP)
- Health card number (SM - Health)
- Driver's license Number/Details (SM - Transport)
- Address Details (SM)
- Social Insurance Number (ESDC)
- Passport Number (IRCC)

- First Name (VSO)
- Surname (VSO)
- Gender (VSO)
- Date of Birth (VSO)
- Date of Death (VSO)
- Citizenship Status (IRCC)
- Residential Status (IRCC)
- Birth certificate document number (VSO)
- Effective date of address change (SM - Health/Transport)
- Address Details (SM)
- Social Insurance Number (ESDC)

- Citizenship Status
- Residential Status

ESDC-SIN-EP: ESDC – SIN Enabled Program

#### Workflow



#### Legal Authority

- ☒ Section 241 of the Income Tax Act (ITA) - Disclosure
- ☒ Section 220 of the ITA - Collection of death info
- ☒ Section 220(1) of the ITA - Collection of SIR data
- ☒ Privacy Act
- ☒ User Consent on T1 to share w/ Elections Canada (EC Act)

#### Security Level

Protected B

#### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T Service Ministries
- ☒ IRCC (Citizenship/Residency)
- ☒ ESDC (Social Insurance Registry)

LAST UPDATED: 16/02/21

Business Line Name

## Employment Insurance Program

Department/Agency

Employment and Social Development Canada  
(ESDC)

## Service Offering

Employment Insurance (EI) provides temporary financial assistance to unemployed Canadians who have lost their job through no fault of their own, while they look for work or upgrade their skills.

ESDC's EI Program would use CDI to enhance the validation of an individual as they create an EI account in Appli-Web. CDI would allow EI to **use a secondary source of identity information** to validate an individual's identity prior to an account being completed.

**It is important for EI to connect to CDI in order to properly validate the identity of an individual and leverage P-T VSO/SM information to improve the integrity of its data.**

## Functionality Type

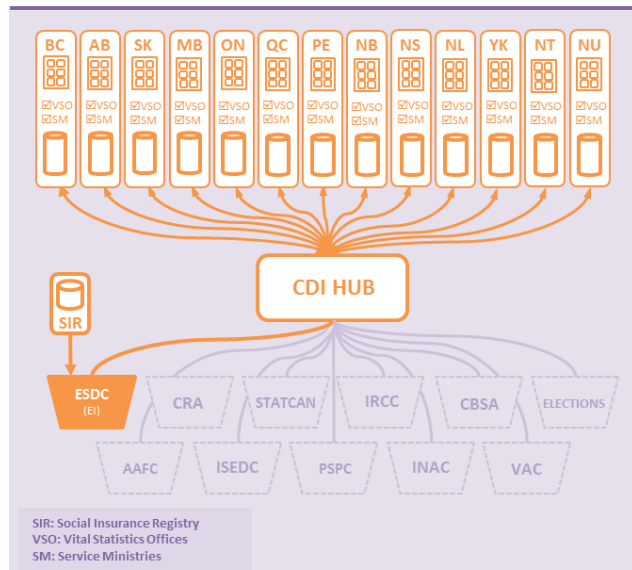
1 Validation	2 Notification	3 Retrieval
Support the individual validation of clients using the Social Insurance Registry (SIR) with a second authoritative source (Driver's License).	Receipt of Death Notifications from P-T VSOs, and address information changes from P-T SMs.	
TBD	TBD	

## Data Attributes

<ul style="list-style-type: none"> <li>First Name (ESDC-SIN-EP)</li> <li>Surname (ESDC-SIN-EP)</li> <li>Date of Birth (ESDC-SIN-EP)</li> <li>Driver's license number/information (SM - Transport)</li> <li>Address Details (SM - Transport/Health)</li> </ul>	<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Date of Death (VSO)</li> <li>Effective date of address change (SM - Health/Transport)</li> </ul>	
---	--	--

ESDC-SIN-EP: ESDC – SIN Enabled Program

## Workflow



## Legal Authority

- ☒ Department of Employment & Skills Development Act
- ☒ Employment Insurance Act
- ☒ Privacy Act

## Security Level

Protected B

## Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs (P-T Ministry of Transport)
- ☒ ESDC (Social Insurance Registry)

LAST UPDATED: 16/02/21



Business Line Name

Job Bank

Department/Agency

Employment and Social Development Canada  
(ESDC)

#### Service Offering

Job Bank is the Government of Canada's leading source for jobs and labour market information. It offers users free occupational and career information such as job opportunities, educational requirements, main duties, wage rates and salaries, current employment trends, and outlooks.

Job Bank currently uses a custom registration log-in solution for client identity management to access Job Match and the Job Bank for Employers service. Job Bank is slated to adopt ESDC's Enterprise Cyber Authentication Solution (ECAS) in the future. **Job Bank would benefit from a CDI connection in order to support the proper validation of the identity of an individual.**

#### Functionality Type

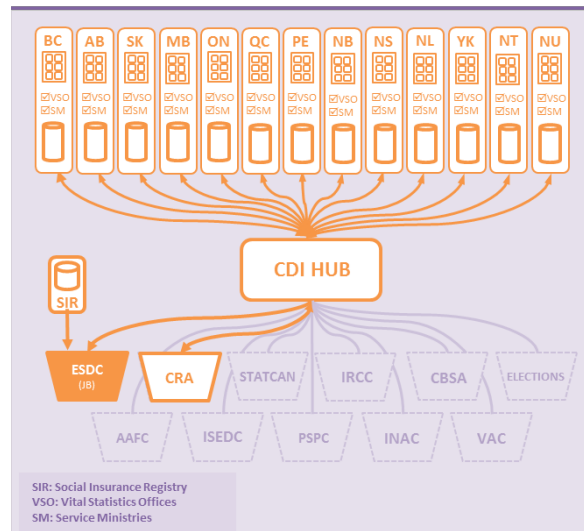
1 Validation	2 Notification	3 Retrieval
Support the individual validation of clients using the Social Insurance Registry (SIR) with a second authoritative source (Driver's License). Validate Business Numbers against CRA data.	Receipt of <i>Death Notifications</i> from P-T VSOs.  Receipt of Deactivated or inactive Business Numbers (CRA) from CRA	Retrieve business information from CRA.
~150,000 per year	TBD	TBD

#### Data Attributes

<ul style="list-style-type: none"> <li>First Name (ESDC-SIN-EP)</li> <li>Surname (ESDC-SIN-EP)</li> <li>Date of Birth (ESDC-SIN-EP)</li> <li>Driver's license number/information (SM - Transport)</li> <li>Social Insurance Number (ESDC)</li> <li>Mother's Maiden Name (ESDC)</li> </ul>	<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Date of Death (VSO)</li> <li>Deactivated or inactive Business Numbers (CRA)</li> </ul>	<ul style="list-style-type: none"> <li>Business Number (CRA)</li> <li>First Name of Business Owner (CRA)</li> <li>Surname of Business Owner (CRA)</li> <li>Account Status (CRA)</li> <li>Business Name (CRA)</li> <li>Operating Name (CRA)</li> <li>Industrial Sector (CRA)</li> <li>Website URL (CRA)</li> <li>Size of Business (CRA)</li> <li>Mailing Information (CRA)</li> <li>Phone Number (CRA)</li> <li>Email Address (CRA)</li> </ul>
---	--	---

ESDC-SIN-EP: ESDC – SIN Enabled Program

#### Workflow



#### Legal Authority

- ☒ Department of Employment & Skills Development Act
- ☒ Employment Insurance Act

#### Security Level

Protected B

#### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs (P-T Ministry of Transport)
- ☒ ESDC (Social Insurance Registry)
- ☒ CRA (Business Numbers)

LAST UPDATED: 16/02/21

Business Line Name

## Record of Employment (ROE)

Department/Agency

## Employment and Social Development Canada (ESDC)

### Service Offering

A Record of Employment (ROE) provides information on employment history. It is the single most important document used by employees in establishing a claim for Employment Insurance (EI) benefits.

Service Canada uses the information on the ROE to determine whether a person is eligible to receive EI benefits, what the benefit amount will be, and for how long the benefits will be paid.

**ROE uses ECAS as their login solution which is used for identity management that would benefit from CDI and leverage P-T VSO/SM information to improve the integrity of its data.**

### Functionality Type

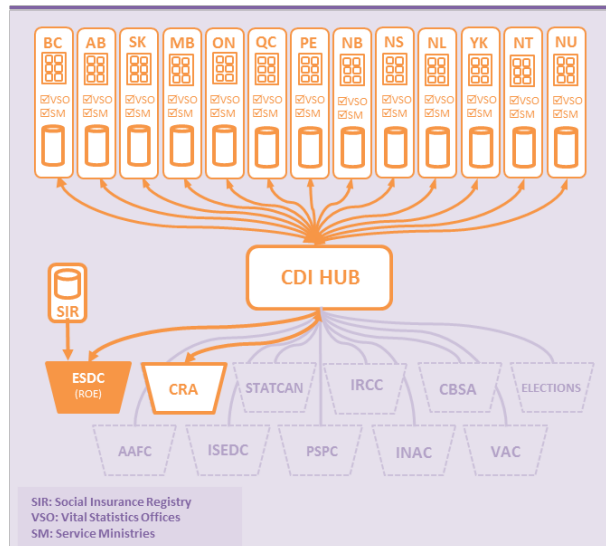
1 Validation	2 Notification	3 Retrieval
Validate individual using the Social Insurance Registry (SIR) and a second authoritative source (Driver's).  Validate Business Numbers against CRA data	Receipt of Death Notifications from P-T VSOs, and address information changes from P-T SMs. Receipt of deactivated or inactive business activities notifications from CRA	Retrieve business information from CRA.
TBD	TBD	TBD

### Data Attributes

<ul style="list-style-type: none"><li>First Name (ESDC-SIN-EP)</li><li>Surname (ESDC-SIN-EP)</li><li>Date of Birth (ESDC-SIN-EP)</li><li>Driver's license number/information (SM - Transport)</li><li>Social Insurance Number (ESDC)</li><li>Mother's Maiden Name (ESDC)</li></ul>	<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Date of Death (VSO)</li><li>Deactivated or inactive Business Numbers (CRA)</li></ul>	<ul style="list-style-type: none"><li>Business Number (CRA)</li><li>First Name of Business Owner (CRA)</li><li>Surname of Business Owner (CRA)</li><li>Account Status (CRA)</li></ul>
--	---	---

ESDC-SIN-EP: ESDC – SIN Enabled Program

### Workflow



### Legal Authority

- ☒ Department of Employment & Skills Development Act
- ☒ Employment Insurance Act

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs (Ministry of Transport)
- ☒ ESDC (Social Insurance Registry)
- ☒ CRA (Business Numbers)

LAST UPDATED: 16/02/21

Business Line Name

Canada Pension Plan (CPP)

Department/Agency

Employment and Social Development Canada  
(ESDC)

### Service Offering

The CPP provides pensions and benefits when contributors retire, become disabled, or die.

CPP uses ECAS as their login solution which is used for identity management that would benefit from CDI.

**It is important for CPP to connect to CDI in order to properly validate the identity of an individual and leverage P-T VSO/SM information to improve the integrity of its data.**

### Functionality Type

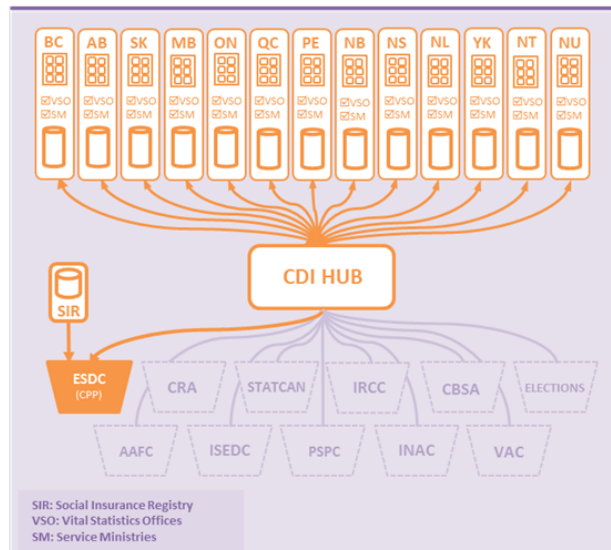
1 Validation	2 Notification	3 Retrieval
Validate individual using the Social Insurance Registry (SIR) and a second authoritative source (Driver's).	Receipt of Death Notifications from P-T VSOs.	
TBD	TBD	

### Data Attributes

<ul style="list-style-type: none"><li>First Name (ESDC-SIN-EP)</li><li>Surname (ESDC-SIN-EP)</li><li>Date of Birth (ESDC-SIN-EP)</li><li>Driver's license number/information (SM - Transport)</li><li>Social Insurance Number (ESDC)</li><li>Mother's Maiden Name (ESDC)</li></ul>	<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Date of Death (VSO)</li></ul>	
--	--	--

ESDC-SIN-EP: ESDC – SIN Enabled Program

### Workflow



### Legal Authority

- ☒ Department of Employment & Skills Development Act
- ☒ Employment Insurance Act

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs (Ministry of Transport)
- ☒ ESDC (Social Insurance Registry)

LAST UPDATED: 16/02/21

Business Line Name

Old Age Security (OAS)

Department/Agency

Employment and Social Development Canada  
(ESDC)

### Service Offering

The Old Age Security (OAS) pension is a monthly payment available to most people 65 years of age and older who meet the Canadian legal status and residence requirements.

CPP uses ECAS as their login solution which is used for identity management that would benefit from CDI.

**It is important for CPP to connect to CDI in order to properly validate the identity of an individual and leverage P-T VSO/SM information to improve the integrity of its data.**

### Functionality Type

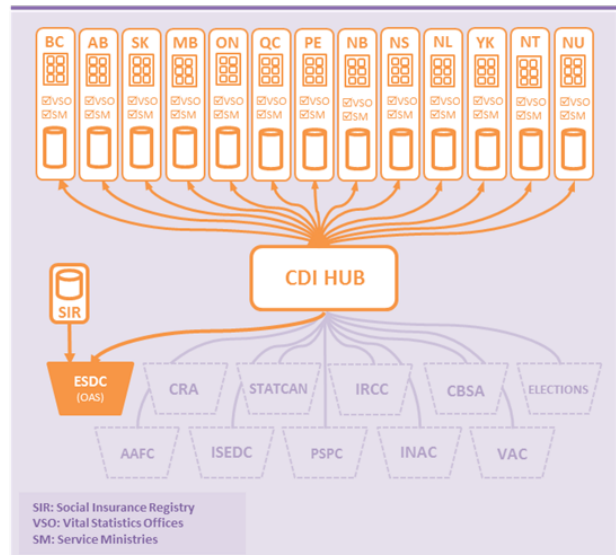
1 Validation	2 Notification	3 Retrieval
Validate individual using the Social Insurance Registry (SIR) and a second authoritative source (Driver's).	Receipt of <i>Death Notifications</i> from P-T VSOs.	
TBD	TBD	

### Data Attributes

<ul style="list-style-type: none"><li>First Name (ESDC-SIN-EP)</li><li>Surname (ESDC-SIN-EP)</li><li>Date of Birth (ESDC-SIN-EP)</li><li>Driver's license number/information (SM - Transport)</li><li>Social Insurance Number (ESDC)</li><li>Mother's Maiden Name (ESDC)</li></ul>	<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Date of Death (VSO)</li></ul>	
--	--	--

ESDC-SIN-EP: ESDC – SIN Enabled Program

### Workflow



### Legal Authority

- ☒ Department of Employment & Skills Development Act
- ☒ Employment Insurance Act

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ ESDC (Social Insurance Registry)
- ☒ P-T SMs (Ministry of Transport)

LAST UPDATED: 16/02/21

Business Line Name

## Immigration Program: Permanent Resident Applications

Service Offering

Issuance of **Permanent Residence** to an individual who has a right to it.

CDI will assist in **increasing the integrity of the overall issuance process** by allowing for the real-time electronic validation of *P-T Birth Registration/ Certificate Information* (of individuals who wish to sponsor someone for permanent residence) with the respective issuing agencies (P-T VSOs).

CDI will allow for the **receipt of electronic Death Notifications** from P-T VSOs which will assist in cancelling related Immigration Documents.

### Functionality Type

1 Validation	2 Notification	3 Retrieval
Validation of P-T <i>Birth Registration or Certificate Information</i> with P-T VSOs.	Receipt of <i>Death Notifications</i> from P-T VSOs.	
650,000 per year	300,000 per year	

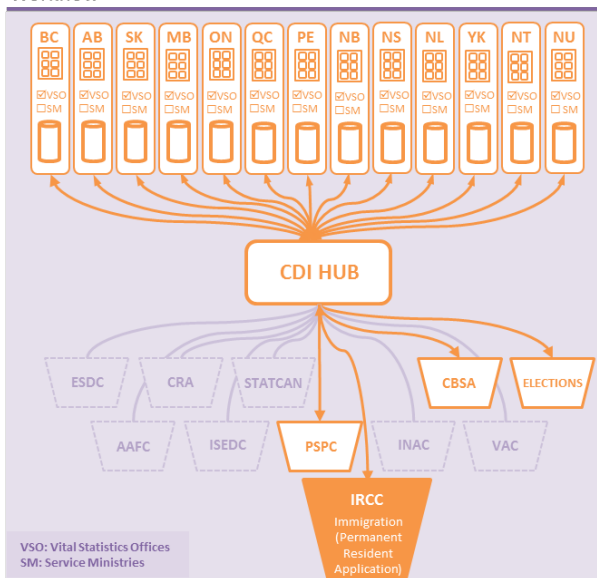
### Data Attributes

<ul style="list-style-type: none"> <li>Birth Certificate Doc. No. (VSO)</li> <li>Birth Certificate Date of Issue (VSO)</li> <li>Birth Registration Number (VSO)</li> <li>Birth Registration Date (VSO)</li> <li>Surname (VSO)</li> <li>Given Name(s) (VSO)</li> <li>Date of Birth (VSO)</li> <li>Gender (VSO)</li> <li>Place of Birth (VSO)</li> <li>Parent's Names/Dates of Birth (VSO)</li> <li>Is individual deceased? (VSO)</li> <li>Is Birth Event valid? (VSO)</li> <li>Is a Legal Name Change associated with the individual? (VSO)</li> <li>Is a Sex Change associated with the individual? (VSO)</li> <li>Is the document lost or stolen? (VSO)</li> </ul>	<ul style="list-style-type: none"> <li>Surname (VSO)</li> <li>Given Name(s) (VSO)</li> <li>Date of Birth (VSO)</li> <li>Gender (VSO)</li> <li>Death Registration Number (VSO)</li> <li>Date of Death (VSO)</li> <li>Place of Death (VSO)</li> </ul>	
---	---	--

Department/Agency

## Immigration, Refugees and Citizenship Canada (IRCC)

### Workflow



### Legal Authority

- ☒ Immigration and Refugee Protection Act
- ☒ Privacy Act

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ Elections Canada
- ☒ CRA
- ☒ PSPC
- ☒ CBSA

LAST UPDATED: 16/02/21

Business Line Name  
Passport Program

Department/Agency  
Immigration, Refugees and Citizenship Canada  
(IRCC)

Service Offering

**Processing of Canadian Passport applications:** the issuance of an internationally respected travel document.

CDI will assist in **increasing the integrity of the overall passport issuance process** by allowing for the real-time electronic validation of P-T Birth Registration/Certificate Information with the respective issuing agencies (P-T VSOs).

CDI will allow for the **receipt of electronic Death Notifications** from P-T VSOs which will assist in *updating the status of related passports*.

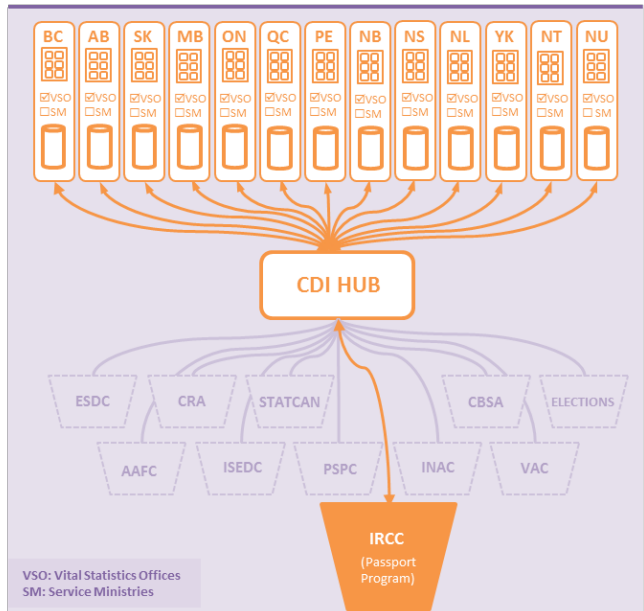
Functionality Type

1 Validation	2 Notification	3 Retrieval
Validation of P-T Birth Registration or Certificate Information with P-T VSOs.	Receipt of Death Notifications from P-T VSOs.	
1.8M (2018-2023) per year 4.2M (2024-2029) per year	300,000 per year	

Data Attributes

<ul style="list-style-type: none"><li>Birth Certificate Doc. No. (VSO)</li><li>Birth Certificate Date of Issue (VSO)</li><li>Birth Registration Number (VSO)</li><li>Birth Registration Date (VSO)</li><li>Surname (VSO)</li><li>Given Name(s) (VSO)</li><li>Date of Birth (VSO)</li><li>Gender (VSO)</li><li>Place of Birth (VSO)</li><li>Parent's Names/Dates of Birth (VSO)</li><li>Is individual deceased? (VSO)</li><li>Is Birth Event valid? (VSO)</li><li>Is a Legal Name Change associated with the individual? (VSO)</li><li>Is a Sex Change associated with the individual? (VSO)</li><li>Is the document lost or stolen? (VSO)</li></ul>	<ul style="list-style-type: none"><li>Surname (VSO)</li><li>Given Name(s) (VSO)</li><li>Date of Birth (VSO)</li><li>Gender (VSO)</li><li>Death Registration Number (VSO)</li><li>Date of Death (VSO)</li><li>Place of Death (VSO)</li></ul>	
---	---	--

Workflow



Legal Authority

- ☒ Canadian Passport Order
- ☒ Privacy Act

Security Level

Protected B

Authoritative Source / Relying Party

- ☒ P-T VSOs

LAST UPDATED: 16/02/21

Business Line Name  
Citizenship Program

Department/Agency  
Immigration, Refugees and Citizenship Canada  
(IRCC)

Service Offering

Processing of **Canadian Citizenship applications** for individuals **born outside of Canada** who have at least one parent who is a Canadian Citizen (issuance of a Canadian Citizenship Certificate to an individual who has a right to it).

CDI will assist in **increasing the integrity of the overall issuance process** by allowing for the real-time electronic validation of parental P-T Birth Registration/ Certificate Information with the respective issuing agencies (P-T VSOs).

CDI will allow for the **receipt of electronic Death Notifications** from P/T VSOs which will assist in **invalidating related Citizenship Certificates**.

Functionality Type

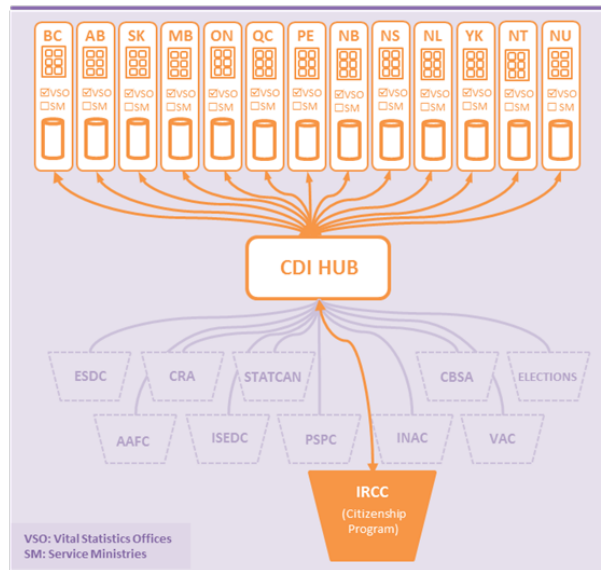
1 Validation	2 Notification	3 Retrieval
Validation of P-T Birth Registration or Certificate Information with P-T VSOs.	Receipt of Death Notifications from P-T VSOs.	
50,000 per year	300,000 per year	

Data Attributes

- Birth Certificate Doc. No. (VSO)
- Birth Certificate Date of Issue (VSO)
- Birth Registration Number (VSO)
- Birth Registration Date (VSO)
- Surname (VSO)
- Given Name(s) (VSO)
- Date of Birth (VSO)
- Gender (VSO)
- Place of Birth (VSO)
- Parent's Names/Dates of Birth (VSO)
- Is individual deceased? (VSO)
- Is Birth Event valid? (VSO)
- Is a Legal Name Change associated with the individual? (VSO)
- Is a Sex Change associated with the individual? (VSO)
- Is the document lost or stolen? (VSO)

- Surname (VSO)
- Given Name(s) (VSO)
- Date of Birth (VSO)
- Gender (VSO)
- Death Registration Number (VSO)
- Date of Death (VSO)
- Place of Death (VSO)

Workflow



Legal Authority

- ☒ Citizenship Act
- ☒ Privacy Act

Security Level

Protected B

Authoritative Source / Relying Party

- ☒ P-T VSOs

LAST UPDATED: 16/02/21

Business Line Name

## Multiple Social and Economic Statistical Programs

Service Offering

Statistics Canada is interested in receiving data to benefit to any of Statistics Canada's many statistical programs, both social and economic. Statistics Canada's mandate is focused on the collection of statistical information on the Canadian population either through the use of administrative data or from survey respondents directly.

As CDI will initially be an identity validation initiative, **Statistics Canada would be interested in receiving data from F/P-T CDI partners related to events such as name changes, marital status, gender change, etc. Once all F/P-T needs have been collected, CBS would like to review the findings to see which elements would be available through CDI.**

Functionality Type

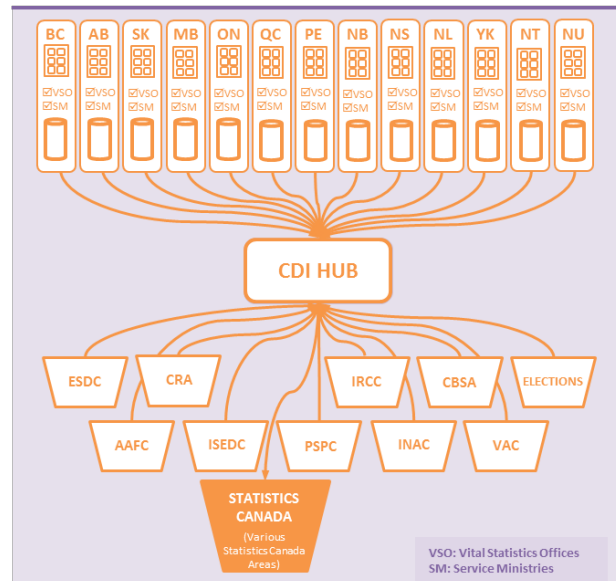
1 Validation	2 Notification	3 Retrieval
	Receipt of Birth and Death Notifications from P-TVSOs.	Statistics Canada is interested in any/all data that can be retrieved from all Federal Departments/P-TVSOs and SMs.
	TBD	TBD

Data Attributes

	<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Gender (VSO)</li><li>Date of Birth (VSO)</li><li>Citizenship Status (VSO)</li><li>Residential Status (VSO)</li><li>Address Details (SM)</li><li>Etc...</li></ul>	<ul style="list-style-type: none"><li>TBD (will depend on what is available from F/P-T CDI partners)</li></ul>
--	---	--

Department/Agency  
Statistics Canada  
(STATCAN)

Workflow



Legal Authority

- ☒ Statistics Canada Act, s. 13  
Collection only - No disclosure

Security Level

Protected B and lower

Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ All Federal Departments
- ☒ P-T SMs

LAST UPDATED: 16/02/21



Business Line Name  
**Agri-Stability**

Department/Agency  
**Agriculture and Agri-Food Canada  
 (AAFC)**

Service Offering

Agri-Stability is part of the federal, provincial, territorial suite of *Business Risk Management programs*. The Program provides support when producers experience a large margin decline in a farm operation. It requires producers to be proactive about their risk management strategy and enroll early in their production year. Program payments are based on the entire farm operation. This means that, when determining eligibility, losses in one crop enterprise within the operation are offset by gains in another. A portion is administered by P-Ts (BC, AB, SK, ON, QC and PE). Farm operations in other areas are supported directly from the federal government (AAFC). **CDI will allow the administration to confirm date of death sooner and ensure quicker closing of the account and/or payment to the estate/beneficiary.**

Functionality Type

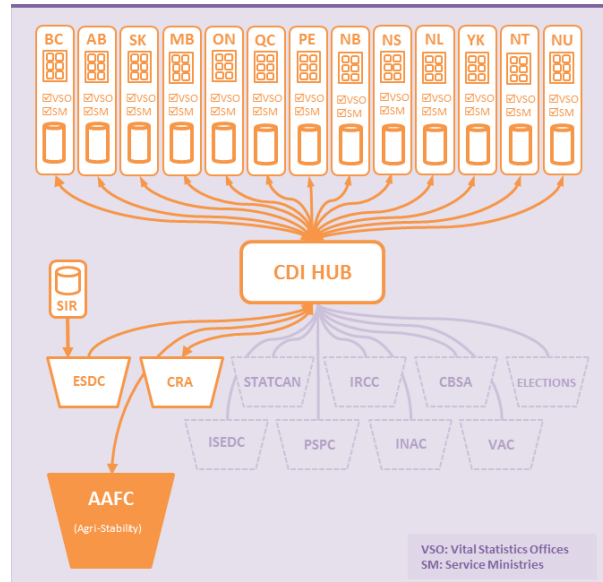
1 Validation	2 Notification	3 Retrieval
Validation of the Personal Identifier Number (PIN) used by AAFC with ESDC SIN	Receipt of Death Notification from P-Ts	
8.000 per year	Death: 270k per year	

Data Attributes

<ul style="list-style-type: none"> <li>First Name (ESDC-SIN-EP)</li> <li>Surname (ESDC-SIN-EP)</li> <li>Address Details (SM)</li> <li>Social Insurance Number (ESDC)</li> <li>Business Number (CRA)</li> </ul>	<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Address Details (SM)</li> <li>Social Insurance Number (ESDC)</li> <li>Date of Death (VSO)</li> </ul>	
--	--	--

ESDC-SIN-EP: ESDC – SIN Enabled Program

Workflow



Legal Authority

- ☒ Farm Income Protection Act
- ☒ Privacy Act (not mentioned on questionnaire)

Security Level

Protected B

Authoritative Source / Relying Party

- ☒ ESDC (Social Insurance Register)
- ☒ CRA (Business Number)
- ☒ P-T VSOs (death)
- ☒ P-T SMs (address)

LAST UPDATED: 16/02/21

Business Line Name

Agri-Invest

Department/Agency

Agriculture and Agri-Food Canada  
(AAFC)

Service Offering

The Agri-Invest program is part of the F/P-T suite of Business Risk Management programs.

Producers use the program to proactively build savings in an account that can be drawn upon in periods of low income or to make investments.

CDI will **allow the Agri-Invest program administration 1) to confirm the date of death of a client sooner and 2) ensure quicker closing of the account and/or payment to the estate/beneficiary.**

Functionality Type

1 Validation	2 Notification	3 Retrieval
Validation of the Personal Identifier Number (PIN) used by AAFC with ESDC SIN	Receipt of Death Notification from P-Ts	
130,000 per year	Death: 270k per year	

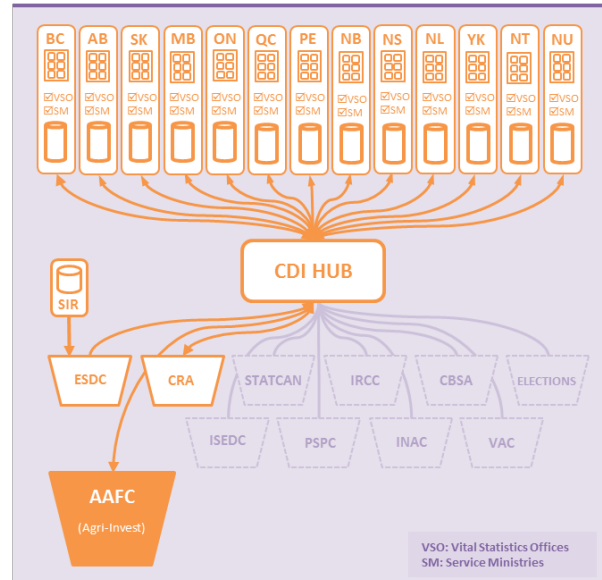
Data Attributes

- First Name (ESDC-SIN-EP)
- Surname (ESDC-SIN-EP)
- Address Details (SM)
- Social Insurance Number (ESDC)
- Business Number (CRA)

- First Name (VSO)
- Surname (VSO)
- Address Details (SM)
- Social Insurance Number (ESDC)
- Date of Death (VSO)

ESDC-SIN-EP: ESDC – SIN Enabled Program

Workflow



Legal Authority

- ☒ Farm Income Protection Act
- ☒ Privacy Act (not mentioned on questionnaire)

Security Level

Protected B

Authoritative Source / Relying Party

- ☒ ESDC (Social Insurance Register)
- ☒ CRA (Business Number)
- ☒ P-T VSOs (death)
- ☒ P-T SMs (address)

LAST UPDATED: 16/02/21

Business Line Name  
Traveller Programs

Department/Agency  
Canada Border Services Agency  
(CBSA)

Service Offering

The CBSA Traveller Programs facilitate the passage of travellers into Canada at the air, land, highway, rail, and marine ports of entry. The Trusted Traveller Programs, under Traveller Programs, are designed to simplify the border clearance process for pre-approved, low-risk travellers entering Canada.

The potential CBSA services that can benefit from the CDI include but are not limited to:

- APEC Business Travel Card (ABTC)
- Commercial Driver Registration Program (CDRP)
- CANPASS suite of programs
- Free and Secure Trade (FAST)
- NEXUS Program
- Remote Area Border Crossing (RABC) Program

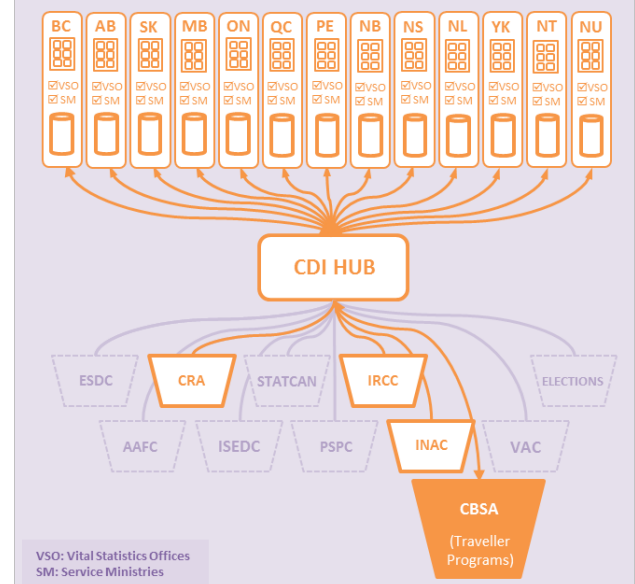
Functionality Type

1 Validation	2 Notification	3 Retrieval
Validate personal information (e.g. individual's legal name, date of birth and home address); Validation of Citizenship/Visa Status from IRCC; Validation of Certificate of Indigenous Status from INAC.	Receipt of Death Notification from P-T VSOs.	
300k per year	Death: TBD	

Data Attributes

<ul style="list-style-type: none"> <li>• First Name (VSO)</li> <li>• Surname (VSO)</li> <li>• Middle Name (VSO)</li> <li>• Date of Birth (VSO)</li> <li>• Birth Certificate (VSO)</li> <li>• City of Birth (VSO)</li> <li>• Country of Birth (VSO)</li> <li>• Home Address (SM)</li> <li>• Postal Code (SM)</li> <li>• Mailing Address (SM)</li> <li>• Gender (VSO)</li> <li>• Driver's license number (SM - Transport)</li> <li>• Passport Number (IRCC)</li> <li>• Immigration Status (IRCC)</li> <li>• Citizenship Status (IRCC)</li> <li>• Permanent Resident Card (IRCC)</li> <li>• Record of Landing (IRCC)</li> <li>• Work Permit (IRCC)</li> <li>• Study Permit (IRCC)</li> <li>• Certificate of Indian Status (INAC)</li> </ul>	<ul style="list-style-type: none"> <li>• First Name (VSO)</li> <li>• Surname (VSO)</li> <li>• Middle Name (VSO)</li> <li>• Address Details (SM)</li> <li>• Date of Death (VSO)</li> </ul>	
--	---	--

Workflow



Legal Authority

- ☒ Customs Act
- ☒ Immigration and Refugee Protection Act

For Disclosure: New Authorities may be required

Security Level

Protected B

Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs
- ☒ IRCC (Citizenship & Visa Status - GCMS)
- ☒ INAC (Secure Certificate of Indian Status)
- ☒ Canada Revenue Agency (CRA)

LAST UPDATED: 25/02/21

Business Line Name

## Commercial Programs

Department/Agency

Canada Border Services Agency  
(CBSA)

### Service Offering

Commercial Programs provide services to a variety of recipients, including businesses (e.g. importers, exporters, carriers, freight forwarders, customs brokers, duty free shop operators, warehouse operators, and more), Government of Canada departments/agencies, and many other stakeholders impacted by international trade. Services include providing resources, advisory services, regulatory/compliance enforcement, and rule making related to development, maintenance, and administration of commercial policies, procedures, regulations, and legislation related to the movement of commercial goods into, through, and out of Canada.

Commercial Programs can leverage the technological capacity provided by the CDI to further simplify import border requirements so that low-risk shipments can be processed more quickly and efficiently at the border. Increased facilitation, in addition to saving businesses time and money, will allow CBSA to better focus its resources on identifying high-risk shipments that pose a potential threat to the health, safety or economic well-being of Canadians.

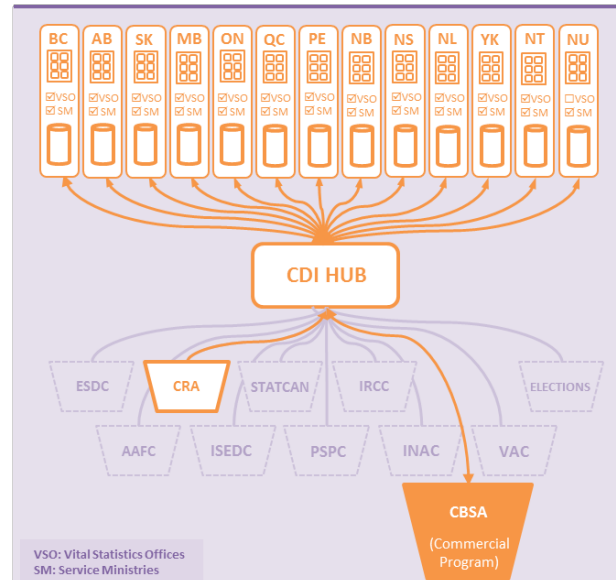
### Functionality Type

1 Validation	2 Notification	3 Retrieval
Validation of business information for programs such as Carrier Code, Trusted Trader and Electronic Data Interchange applications.	Receipt of address changes notifications from P-T SMs; Receipt of bankruptcy and merger/acquisition notifications from the CRA.	
TBD	TBD	

### Data Attributes

<ul style="list-style-type: none"><li>Business Number (CRA)</li><li>Legal Business Name (CRA)</li><li>Operating Name (CRA)</li><li>Business Address (CRA)</li><li>Mailing Address (CRA)</li></ul>	<ul style="list-style-type: none"><li>Address Change (SM)</li><li>Bankruptcy (CRA)</li><li>Merger/acquisition (CRA)</li></ul>	
<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Home Phone Number (SM)</li><li>Employer Name (CRA)</li><li>E-mail Address (SM)</li></ul>		

### Workflow



### Legal Authority

- ☒ Customs Act
  - ☒ Immigration and Refugee Protection Act
- For Disclosure: New Authorities may be required

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs
- ☒ CRA

LAST UPDATED: 25/02/21

Business Line Name

## Enforcement & Intelligence Ministerial Relief

Service Offering

Under the *Immigration and Refugee Protection Act (IRPA)*, individuals who are inadmissible to Canada on grounds of security, certain provisions related to human or international rights violations, or organized criminality may request that the Minister of Public Safety and Emergency Preparedness grant them relief from their inadmissibility on the basis that it would not be contrary to the national interest. This process is referred to as "Ministerial Relief".

CDI has the potential to assist validation of an individual to facilitate client identity management and authorities for the "Enforcement & Intelligence Ministerial Relief" Program.

### Functionality Type

1 Validation	2 Notification	3 Retrieval
Validate personal information such as the individual's legal name and date of birth.	Receipt of Death Notification from P-T VSOs.	
TBD	TBD	

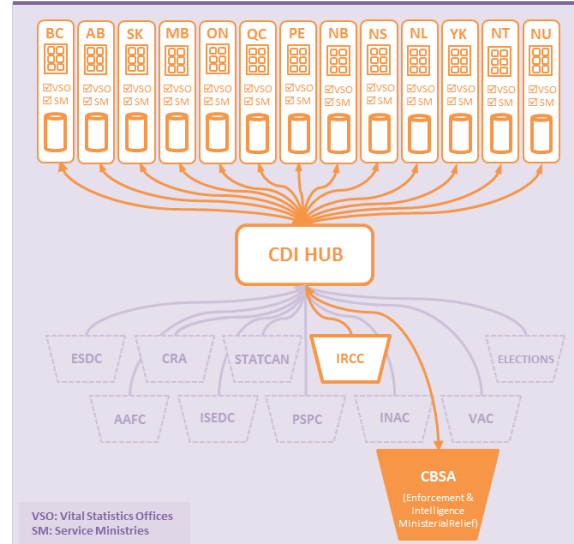
### Data Attributes

<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Middle Name (VSO)</li><li>Date of Birth (VSO)</li><li>City of Birth (VSO)</li><li>Country of Birth (VSO)</li><li>Gender (VSO)</li><li>Address (SM)</li><li>Postal Code (SM)</li><li>Home Phone Number (SM)</li><li>Cell Phone (SM)</li><li>Work Phone (SM)</li><li>E-mail Address (SM)</li><li>Immigration Status (IRCC)</li></ul>	<ul style="list-style-type: none"><li>Date of Death (VSO)</li></ul>	
---	---	--

Department/Agency

## Canada Border Services Agency (CBSA)

### Workflow



### Legal Authority

- ☒ Customs Act
- ☒ Immigration and Refugee Protection Act

For Disclosure: New Authorities may be required

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSOs
- ☒ P-T SMs
- ☒ IRCC (Citizenship & Visa Status - GCMS)

LAST UPDATED: 25/02/21

## Business Line Name

# National Register of Electors (NRoE)

## Department/Agency Elections Canada (EC)

### Service Offering

NRoE is a database of over 30 million people that is constantly maintained via various bulk data sources including CRA, IRCC (new citizens), P-T Drivers License bureaus, 13 P-T VSOs, and 13 P-T Electoral Management Body partnerships (e.g.: Elections Ontario).

It is critical that the NRoE is kept up-to-date regarding **name**, **address**, **date-of-birth**, and **citizenship** as these determine eligibility and location for voting purposes. Life change events are also very important as they capture **deaths**, **name changes**, and **gender changes**. Finally, EC is interested in identifying and **activating citizens** or **removing non-citizens** from the NRoE.

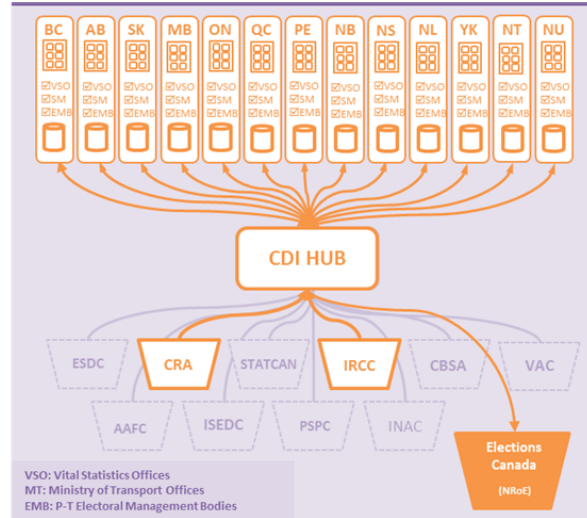
### Functionality Type

1 Validation	2 Notification	3 Retrieval
Validate birth and citizenship details for potential electors in order to improve the quality of the NRoE.	Receive notifications of life change events such as becoming an adult, name change and deaths in order to better maintain the NRoE.	
TBD	TBD	

### Data Attributes

<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Gender (VSO)</li> <li>Date of Birth (VSO)</li> <li>Date of Death (VSO)</li> <li>Country of Birth (VSO)</li> <li>Date of Citizenship Attribution (IRCC)</li> <li>Date of Citizenship Revocation (IRCC)</li> <li>Address Details (SM-Transport/CRA)</li> <li>Electoral participants data (EMB if someday connected to PT HUB)</li> </ul>	<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Death Notification (VSO)</li> <li>Citizenship Status (IRCC)</li> <li>Death Notification (VSO)</li> <li>New Citizens/Electors (18 years old) (IRCC)</li> <li>Residential address (SM/CRA)</li> <li>Mailing address (SM/CRA)</li> <li>Date of Birth (VSO)</li> <li>Gender Change (VSO)</li> <li>Driver's Licence data (SM)</li> <li>Name change (VSO)</li> <li>Gender change (VSO)</li> <li>Date of Citiz Attribution (IRCC)</li> <li>Date of Citiz Revocation (IRCC)</li> </ul>	
--	--	--

### Workflow



### Legal Authority

<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Canada Elections Act</li> <li><input checked="" type="checkbox"/> Federal data sharing agreements w/IRCC and CRA</li> </ul>	<h3>Security Level</h3> <p>Protected B</p>
--	--

### Authoritative Source / Relying Party

<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> P-T VSOs</li> <li><input checked="" type="checkbox"/> IRCC</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> CRA</li> <li><input checked="" type="checkbox"/> P-T SMs</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> P-T EMB</li> </ul>
--	--	---

LAST UPDATED: 16/02/21

Business Line Name

## Registration and Membership (incl. Secure Certificate of Indian Status)

Service Offering

Registration of First Nation individuals entitles them access to programs services and issuance of a Secure Certificate of Indian Status. Credential and identity validations are required using an authoritative source, currently the long form birth certificate issued by P/T VSOs across the country, to deliver on all its services.

CDI would offer an automated, secure, efficient and fast alternative to the current paper-based system. It would generate economies of time for the government and improve service for clients. It would also provide a fast alternative to clients in remote location who have no regular mail service and for whom it is a large burden to request paper birth certificate from their P/T government.

### Functionality Type

1 Validation	2 Notification	3 Retrieval
Validation of First Nations Individual so they can benefit from programs and services offered strictly to First Nations. Note that they may be a Non-Canadian born individual.	Death notifications Birth notifications	Retrieval of long form birth for the individual to determine lineage (Registration or SCIS)
~145,000 per year	Birth: N/A Death: ~5500	

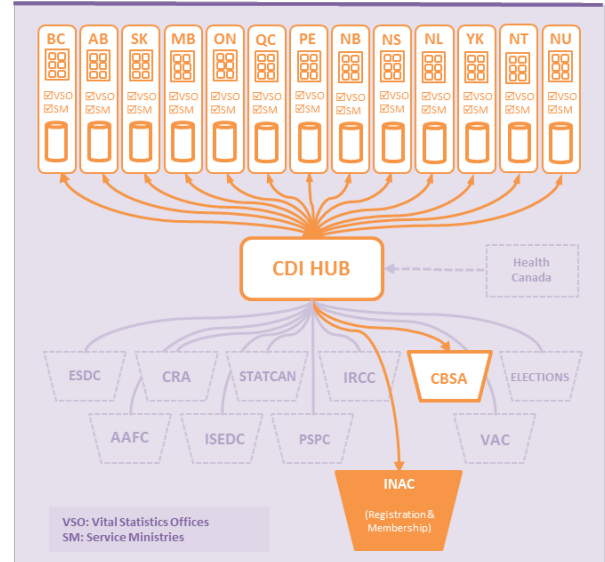
### Data Attributes

<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Gender (VSO)</li> <li>Date of Birth (VSO)</li> <li>Applicant Name (VSO)</li> <li>Applicant Date of Birth (VSO)</li> <li>Mother Name (VSO)</li> <li>Mother Date of Birth (VSO)</li> <li>Mother Name at Birth (VSO)</li> <li>Father Name (VSO)</li> <li>Father Date of Birth (VSO)</li> <li>Birth Location (VSO)</li> <li>Marriage Certificate (VSO)</li> <li>(Birth) Name of Bride (VSO)</li> <li>Name of Groom (VSO)</li> <li>Date of Marriage (VSO)</li> <li>Registration Number (VSO)</li> <li>Place of Marriage (VSO)</li> <li>Name change (VSO)</li> <li>Adoptions (VSO)</li> </ul>	<ul style="list-style-type: none"> <li>Death Notification (VSO)</li> <li>Birth Notifications (VSO)</li> </ul>	<ul style="list-style-type: none"> <li>Long form Birth Certificate data required to determine lineage (VSO)</li> </ul>
---	---	--

Department/Agency

## Indigenous and Northern Affairs Canada (INAC)

### Workflow



### Legal Authority

- ☒ DIAND Act, s. 4
- ☒ Indian Act section s. 5, s. 9, s. 42

### Security Level

Protected B

### Authoritative Source / Relying Party

- ☒ P-T VSO/SM
- ☒ CBSA

LAST UPDATED: 16/02/21

Business Line Name  
Receiver General

Department/Agency  
Public Services and Procurement Canada  
(PSPC)

#### Service Offering

The Receiver General issues in excess of 300 million annual payments on behalf of federal departments and some provincial governments. The Receiver General is presently undergoing a transformation initiative to improve the processes and systems used in the delivery of its services to departments and Canadians.

As part of this transformation, it is possible that the Receiver General may choose to centralize the *capture, distribution or storage of payee data*. Should any of these models occur, the **Receiver General could leverage CDI to assist with the validation of individuals upon registering or with the notification of life events**.

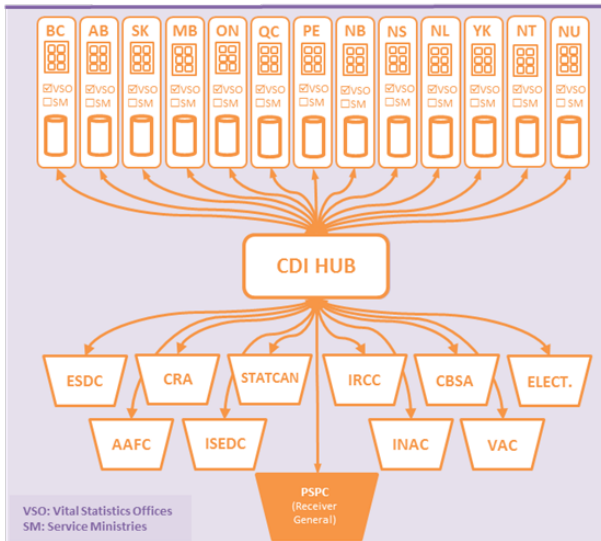
#### Functionality Type

1 Validation	2 Notification	3 Retrieval
Validation of identity of payee before setting up direct deposit with P-T VSOs.	Receipt of life events (birth, death, etc.) from P-T VSOs and other Federal Depts. Receipt of address information changes from SMs.	
300M annual payments	Death: 270k per year	

#### Data Attributes

<ul style="list-style-type: none"><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Gender (VSO)</li><li>Date of Birth (VSO)</li><li>Applicant Name (VSO)</li><li>Applicant Date of Birth (VSO)</li><li>Mother Name (VSO)</li><li>Mother Date of Birth (VSO)</li><li>Mother Name at Birth (VSO)</li><li>Father Name (VSO)</li><li>Father Date of Birth (VSO)</li><li>Birth Location (VSO)</li><li>Address Details (SM)</li></ul>	<ul style="list-style-type: none"><li>Death Notification (VSO)</li><li>Birth Notifications (VSO)</li><li>First Name (VSO)</li><li>Surname (VSO)</li><li>Gender (VSO)</li><li>Date of Birth (VSO)</li><li>Date of Death (VSO)</li><li>Place of Death (VSO)</li><li>Age of the deceased at the time of death (VSO)</li></ul>	
---	--	--

#### Workflow



#### Legal Authority

☒ New authorities may be required

#### Security Level

Could be Protected A or B, dependent on client identifier associated with payee

#### Authoritative Source / Relying Party

☒ P-T VSOs  
☒ Other Federal Departments

LAST UPDATED: 16/02/21



Business Line Name

Compensation Services: Pay, Pension, Insurance

Department/Agency

Public Services and Procurement Canada  
(PSPC)

### Service Offering

PSPC is Canada's largest payroll and pension administrator. They provide compensation services for federal departments, agencies, and public service pensioners.

To ensure accurate and timely processing of payments and benefits, access to vital statistics information such as birth and death as well as information on marriage status are critical to ensure the proper administration of compensation services. In addition, any changes to this information are critical to ensure that correct monies or benefits are paid or, when required, collected.

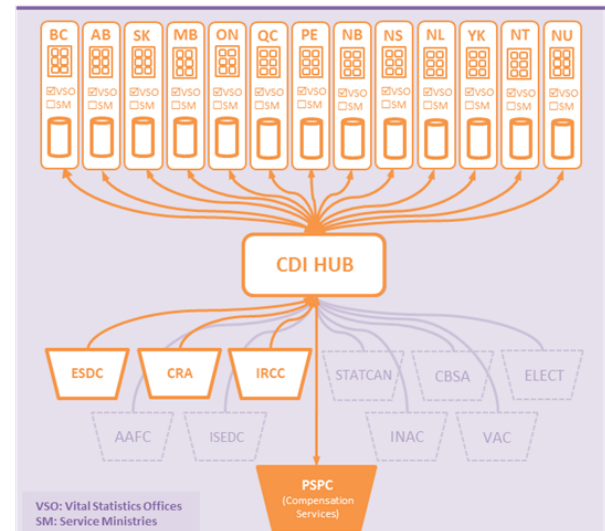
### Functionality Type

1 Validation	2 Notification	3 Retrieval
Setting up of an individual in the compensation systems to ensure that tombstone data is accurate.	Death, Marriage events and/or changes to employment status, benefits or pension options.	CPP Disability benefit details from ESDC to determine how much a client can receive. Survivor Benefits—are children still in school, is there a spouse, etc.
~7.2M/yr	~10K/yr	

### Data Attributes

<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Gender (VSO)</li> <li>Date of Birth (VSO)</li> <li>Applicant Name (VSO)</li> <li>Applicant Date of Birth (VSO)</li> <li>Mother Name (VSO)</li> <li>Mother Name at Birth (VSO)</li> <li>Father Name (VSO)</li> <li>Birth Location (VSO)</li> <li>Address Details (SM)</li> <li>Direct Deposit Information (TBD)</li> </ul>	<ul style="list-style-type: none"> <li>Death Notification (VSO)</li> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Gender (VSO)</li> <li>Date of Birth (VSO)</li> <li>Date of Death (VSO)</li> <li>Place of Death (VSO)</li> <li>Age of the deceased at the time of death (VSO)</li> </ul>	<ul style="list-style-type: none"> <li>Receiving a CPP disability payment (ESDC)</li> </ul>
---	---	---

### Workflow



### Legal Authority

☒ New authorities may be required

### Security Level

Protected B

### Authoritative Source / Relying Party

☒ P-T VSOs  
☒ CRA  
☒ ESDC (Social Insurance Registry, CPP Disability,)  
☒ IRCC  
☒ Family Members

LAST UPDATED: 16/02/21

## Service Offering

VAC collects and uses personal information for the specific purpose of administering and delivering its programs and benefits. It is used specifically for determining program eligibility (e.g.: Identity validation and death notifications). This information is important to ensure that the delivery of any benefit or service is made to the rightful individual: Change of address and Birth of an individual. CDI will **allow VAC to lessen the administrative burden on clients to report changes in circumstances that have already been notified to other government departments**. CDI will also **enable VAC to have current and valid information about a client to ensure benefit eligibility and delivery is accurate and appropriate**.

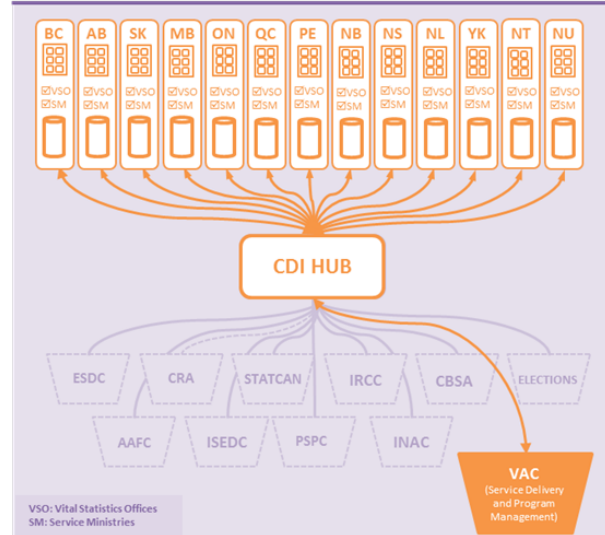
## Functionality Type

1 Validation	2 Notification	3 Retrieval
Validate an individual using a secondary authoritative source with P-T VSO/SM (Min. of Transport/Health).	Notification of death; Change of address; Birth of a dependant;	
7,000 new clients per year	250,000 information change 17,000 client deaths per year	

## Data Attributes

<ul style="list-style-type: none"> <li>Driver's license (SM)</li> <li>Health care card (Excluding Alberta and Manitoba) (SM)</li> <li>Birth certificate (VSO/SM)</li> <li>Marriage certificate (SM)</li> <li>Canadian Passport Data (IRCC)</li> <li>DND Identification Card (DND)</li> <li>DND Casualty Notification (DND)</li> <li>Client's file number or service number (DND)</li> </ul>	<ul style="list-style-type: none"> <li>First Name (VSO)</li> <li>Surname (VSO)</li> <li>Date of Birth (VSO)</li> <li>Date of Death (VSO)</li> <li>Address Details (SM)</li> <li>Date of address change (SM)</li> <li>Status of address change (permanent/temporary) (SM)</li> </ul>	
---	---	--

## Workflow



## Legal Authority

<input checked="" type="checkbox"/> New authorities may be required.
--

## Security Level

Protected B
-------------

## Authoritative Source / Relying Party

<input checked="" type="checkbox"/> P-T VSOs	<input checked="" type="checkbox"/> P-T SMs (Ministry of Transport, Ministry of Health)
--	---

LAST UPDATED: 16/02/21

## ANNEX C – SUMMARY OF CURRENT FEDERAL AUTHORITIES

Department / Agency	Business Line	Business Need (Functionality)	Authoritative Source/ Relying Party
CRA	Individual Identification (Ident) System	✓ Validation ✓ Notification ✓ Retrieval	⇌ P-T VSOs ⇌ ESDC ⇌ IRCC ⇌ P-T SM of Transport ⇌ P-T SM of Health ⇌ Elections Canada
ESDC	Employment Insurance (EI)	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ P-T SM of Transport ⇌ ESDC
ESDC	Job Bank (JB)	✓ Validation ✓ Notification ✓ Retrieval	⇌ P-T VSOs ⇌ P-T SM of Transport ⇌ ESDC ⇌ CRA
ESDC	Record of Employment (ROE)	✓ Validation ✓ Notification ✓ Retrieval	⇌ P-T VSOs ⇌ P-T SM of Transport ⇌ ESDC ⇌ CRA
ESDC	Canada Pension Plan (CPP)	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ P-T SM of Transport ⇌ ESDC
ESDC	Old Age Security (OAS)	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ P-T SM of Transport ⇌ ESDC
IRCC	Immigration Program	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ Elections Canada ⇌ CRA ⇌ CBSA ⇌ PSPC
IRCC	Passport Program	✓ Validation ✓ Notification	⇌ P-T VSOs
IRCC	Citizenship Program	✓ Validation ✓ Notification	⇌ P-T VSOs
STATCAN	Multiple Social and Economic Statistical Programs	✓ Notification ✓ Retrieval	⇌ P-T VSOs ⇌ P-T SMs ⇌ All Federal Departments
AAFC	Agri-Stability	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ ESDC ⇌ CRA
AAFC	Agri-Invest	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ ESDC ⇌ CRA
CBSA	Traveller Program	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ IRCC ⇌ INAC ⇌ CRA
CBSA	Commercial Program	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ P-T SMs ⇌ CRA
CBSA	Enforcement & Intelligence Ministerial Relief	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ P-T SMs ⇌ IRCC
ELECTIONS	National Register of Electors	✓ Validation ✓ Notification	⇌ P-T VSO ⇌ P-T SM ⇌ CRA ⇌ P-T EMB ⇌ IRCC
INAC	Registration and Membership	✓ Validation ✓ Notification ✓ Retrieval	⇌ P-T VSOs ⇌ CBSA
ISED	ISED is eager to become a willing and active participant in the CDI. In the future we anticipate widespread interest in our business lines connecting to the CDI as a means of validating, notifying and retrieving information/data for our digital services. We think at this point there may be a possibility for Corporations Canada and its Business Registry information could as authoritative source of data further expanding the business capabilities to the CDI.		
PSPC	Receiver General	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ Federal Departments
PSPC	Compensation Services: Pay, Pension, Insurance	✓ Validation ✓ Notification ✓ Retrieval	⇌ P-T VSOs ⇌ ESDC (SIN and CPP Disability) ⇌ IRCC ⇌ CRA
VAC	Service Delivery and Program Management	✓ Validation ✓ Notification	⇌ P-T VSOs ⇌ P-T SMs (Ministry of Transport/Health)
Legend: ⇌ Bidirectional ⇌ Received from an Authoritative Party ⇌ Shared with Relying Party			

## **ANNEX D – TEN PRIVACY PRINCIPLES**

This Annex provides an overview of the 10 privacy principles as defined by the Office of the Privacy Commissioner and how each principle is taken into account as part of the privacy framework for the CDI's collection, use and disclosure of personal information.

### **Accountability**

The existence of either jurisdictional exchange or a common interchange does not replace the accountabilities of organizations that hold personal information. Authoritative sources are accountable for the information that they disclose to relying parties. Additionally, all parties continue to be accountable for information that they disclose via the identity notification functionality of the Digital Interchange.

The CDI exchange could be governed by a program that would exist within a department/agency with clear authorities, reporting structures, and Program Activity Architecture.

### **Identifying Purposes**

The information is collected by each party for the purposes of the program that collected it. Identity validation is an important purpose for government in the 21<sup>st</sup> century. If any enabling legislation does not permit the disclosure of personal information for the purposes of validating identity, then this legislation would require amendment.

### **Consent**

For purposes where information is exchanged by CDI partners, 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.

There is a reasonable expectation that access to a benefit or service requires that a program determine eligibility. To do that, identity must first be confirmed. If a person makes an in-person visit to a Service Canada centre, they consent to showing identification to a service agent with the understanding that some "behind the scenes" validation may occur.

While informed consent could be used in some circumstances, they are not appropriate for others. The need for consent is therefore not appropriate in cases where there would be high risk to program integrity resulting from a lack of identity validation.

### **Limiting Collection**

In terms of collecting information from citizens, this initiative would not change either the amount or composition of information collected by programs.

In terms of collecting information for the purposes of validation, only the information that is absolutely necessary will be collected.

### **Limiting use, disclosure, retention**

The information used and disclosed by parties under this initiative would only be used for the purposes of identity validation and determining program eligibility. These uses are those specifically named in

the legislation or regulations of jurisdictions. Furthermore, parties would be restricted to disclosing only the information that they have authority to disclose, and that has been agreed to in the multilateral framework agreement.

Information that is transmitted through the hubs would be transitory and not retained by the hubs themselves. This solution is akin to a post office; therefore, no “central” databases are being created. The exchange should be able to filter who is able to validate various types of information in order to reduce the risk that information is disclosed to an unauthorized organization.

The CDI exchange may, depending on the rules of the jurisdiction, maintain a record that certain information was transmitted for security and auditability reasons. For example,

“John Doe – legal status in Canada – requested by Ministry of Transportation of Ontario, responded to by Citizenship and Immigration Canada on January 31, 2018.” In this example, the response itself (legal status) is not kept by the hub, but a transaction record can be kept for continuity of evidence purposes.

### Accuracy

A key strength of the identity notification functionality of this initiative is that personal information banks/databases would be kept more accurate than at present. When a change of an identity attribute occurs, it can be quickly communicated to other parties that hold similar information, significantly reducing inaccuracies.

Further, information sharing framework agreement would oblige parties to ensure that their data holdings are accurate and up-to-date. The agreement as proposed requires jurisdictions to have data holdings audited for accuracy and security.

### Safeguarding

Access to the CDI Exchange would be strictly controlled. All requests, views and transactions would be logged and monitored for irregular or illegal activity in real time. Access to CDI would require Level II security clearance.

Identity information requests and responses would be encrypted twice – both the transportation protocol of the messages as well as the messages themselves. This means that if in the unlikely scenario that an intruder manages to break the transportation encryption and interception an information packet, there is a very low risk that they would be able to open the message.

As part of the information sharing framework, parties to this initiative would notionally agree to be audited by a third party to ensure the security of their data holdings. This would provide some assurance that the Digital Interchange as a whole is secure.

### Openness

The information sharing framework agreement, which would be available to the public when completed, would specifically list all identity information sharing pathways between jurisdictions in a single place. This would be a significant improvement over the status quo, where information sharing is dictated in bilateral agreements.

### Individual access

Individual access does not change under this initiative; Canadians would still have to apply to individual departments, agencies and ministries to request access to their personal information under the *Privacy Act* or PT privacy legislation.

### Challenging compliance

As mentioned, under the information sharing framework agreement, jurisdictions would be obliged to have their data holdings audited to ensure that they are accurate and secure. Summaries of these audits can be made public; however there may be parts of these audits that must be confidential due to security risks.

## ANNEX E – BEST PRACTICES - NATIONAL AND INTERNATIONAL EXAMPLES

In the development of a governance model for CDI, including the assessment of public and private operation of the CDI service, analysis was undertaken to identify national and international precedent and best practices.

There are several best practices that can be looked at in the context of the governance model for CDI. Many other jurisdictions have developed and implemented identity management policies and have operationalized those policies and initiatives in different ways. Given that CDI is envisioned to be a pan-Canadian initiative, there are also examples of best practices to support multilateral or shared governance approaches.

### Leveraging Existing National Agencies

Many developed countries have a single department or agency that manages identity information on behalf of the entire government; however this is because identity is rarely divided among two levels of government. These departments/agencies often issue national identity cards, an approach to identity management not easily implementable in Canada. Most governments using this model are unitary governments. International examples include:

- Federal Ministry of the Interior of **Germany** – National Identity Card program
- **Swedish** Tax Agency – Identity Card/Swedish Personal Identity Number program
- **Denmark** – The Civil Registration System, which issues the Danish Personal Identification Number, is not the same agency that issues the national digital identity (NemID). Instead, the Agency for Digitisation, which is a portfolio agency of the Ministry of Finance, leads an interdepartmental effort to issue digital IDs and credentials. These services extend beyond those planned for CDI.

Crown corporations are government-owned enterprises, operating at arm's length from the government. They are separate legal entities, wholly-owned by the Crown. In Canada, Canada Post has already introduced a digital identity proofing service that it offers to other businesses, using its wide network of service locations to provide in-person verification. After the identity is verified and stored within Canada Post's systems, future validations against it can be offered in real-time, using a transaction fee payment model.

Internationally, crown corporations have also been used to support digital identity services. L'identité numérique de La Poste (France) offers a verified digital identity service that allows a citizen to access FranceConnect, the secure credential service used to unlock a variety of online services, both public and private. FranceConnect itself is a national government program; La Poste is simply an essential delivery mechanism for it.

The Government of New Zealand (NZ), in conjunction with New Zealand Post, municipal governments and the private banking and insurance industries, has recently launched the RealMe identity verification service. While the service currently remains in the early roll-out stage, it would eventually apply to both federal and local levels of governments as well as private industry.

## **Not-for-Profit Corporations and Private Entities**

There are several national examples where shared-governance corporations have yielded successful results.

The Canadian Institute for Health Information (CIHI) is a shared governance corporation that was established incorporated under the Canada Corporations Act in 1994 as an independent, not-for-profit corporation. CIHI is governed by a 16-member board of directors with representation of FPT governments and non-governmental health-related groups or individuals.<sup>22</sup> It is funded predominantly by the federal government, but its revenues include PT contributions as well. CIHI is often looked to as a successful model of how FPT governments can create a shared governance corporation to manage a shared jurisdiction in Canada.

The Interac Association was founded in 1984 by several financial institutions looking to organize electronic payments in the emerging Automated Banking Machine market. Since 1996, the federal Competition Tribunal<sup>23</sup> oversees the Interac Association's membership agreement (called the "Consent Order"),<sup>24</sup> permitting the de facto monopoly to exist. The Consent Order dictates the structure, governance and fee structure of Interac. In 2012, the Tribunal permitted the Association to restructure into a corporation; this restructuring is expected to occur in 2018.

---

<sup>22</sup> Examples of individuals include hospital administrators or university faculty

<sup>23</sup> The Tribunal is a quasi-judicial body, not an agency of the government

<sup>24</sup> Consent Order originates from Tribunal proceeding *Director of Investigation and Research v. Bank of Montreal*, CT-1995-002: <http://www.ct-tc.gc.ca/CMFiles/0092a38PEW-3102004-3532.pdf>



## ANNEX F – COSTING SPECIFICS

### Federal Interoperability Solution (Federal Hub)

#### Federal Infrastructure Costs

This infrastructure will be used to support information exchange between federal departments/agencies with a central piece of infrastructure.



ELEMENTS	LOW	HIGH
Hardware	\$1,800,000	\$3,600,000
Platform Build	\$ 410,000	\$ 820,000
Software Licensing	\$1,205,000	\$2,410,000
Solution Design	\$ 200,000	\$ 400,000
Federal Infrastructure Cost (GC internal Network connection costs to a Federal Hub)	\$2,626,000	\$5,252,000
Additional Federal Infrastructure Development Costs (e.g.: modifying departmental systems)	TBD	TBD
Security	TBD	TBD
<b>Total</b>	<b>\$6M</b>	<b>\$12.4M</b>

#### Federal Infrastructure Service Costs

Federal service costs are based on the most common high-level business needs reported by federal and provincial partners. Each service that needs to be set up costs \$500K. These business needs equate to services which take the form of a notification or validation/retrieval of select pieces of information.<sup>25</sup>

It is assumed that each department/agency would have one application/solution that needs to have services added to. Further costs to connect internal applications have not been included.

<sup>25</sup> This is based on the development work to set up a service between ESDC's Social Insurance Register and IRCC's Global Case Management System.

Example: ESDC uses an Enterprise Cyber Authentication Solution (ECAS) for users to register for Employment Insurance. This same solution is used for Old Age Security and Canada Pension Plan users but the addition of services would only need to be done once on ECAS.

Required Services to set up for Authoritative Parties	Cost for Service Development	Cost Model
Validation of Immigration and Citizenship Information from IRCC	\$500K	Based on equivalent ESDC Development work (SIR → GCMS) ~500K per CDI Service
Validation of Social Insurance Number information from ESDC	\$500K	
Validation of Indian Status information from INAC	\$500K	
<b>3 Services</b>	<b>\$1.5M</b>	
Required Services to set up for Relying Parties	Cost for Service Development	Cost Model
Validation of Birth information from VSO	\$500K	Based on equivalent ESDC Development work (SIR → GCMS) ~500K per Service
Validation of Birth Certificate information from IRCC	\$500K	
Notification of Birth information from VSO	\$500K	
Notification of Death information from VSO	\$500K	
Validation of Driver's License information from SM	\$500K	
Validation of Health Information from SM	\$500K	
<b>6 Services</b>	<b>\$3M</b>	
<b>Multiplied by 11 Federal Departments/Agencies</b>	<b>\$33M</b>	

## Central Infrastructure

This central infrastructure (CDI Hub) will broker information exchanges between the federal government, PTs (and potentially private organizations). Costing estimates are based on developing a centralized, pan-Canadian infrastructure and to connect partners to that architecture. PT analysis could yield an alternative architecture solution, until that exercise is undertaken this is the only solution which will be costed at this time. These alternative models can only be generated once CDI has a formal mandate to engage stakeholders.



This estimate includes the central infrastructure build and onboarding costs. There are some unknown cost elements which contribute to the budget range. It was derived from comparable hub infrastructure set up by ESDC's Department Service Bus.

A detailed RFI/RFP will need to be completed to obtain updated private sector costs that reflect the chosen architecture. Costs associated with the proposed build:

ELEMENTS	LOW	HIGH
CDI Service Bus		
▪ Hardware	\$ 1,800,000	\$ 3,600,000
▪ Platform Build	\$ 410,000	\$ 800,000
▪ Software Licensing	\$ 1,205,000	\$ 2,410,000
Services Development (17 identified CDI Services)	\$ 5,900,000	\$ 11,800,000
Securing data transportation between provincial and CDI Hub **	\$ 750,000	\$ 1,500,000
Connectivity	\$ 120,000	\$ 240,000
Services Implementation	\$10,300,000	\$20,600,000
<b>Total</b>	<b>\$19.7M</b>	<b>\$39.4M</b>

Note: Operation and maintenance costs have not been included within these figures. Based on comparable projects, there would be an additional cost of 20% added to the figures above to account for these costs.

\*\* This cost assumes that the provinces & Territories will require encryption at the transport layer. GCNet cost estimate of \$68,000.00 per month for 10 provincial connections for the first five years not included above. Estimate doesn't include three territories (YK, NWT, NT). These connections do not exist for GCNet, and would cost about two million each to add to those locations. Also assumes two Network to Network Interface (NNI's) will have already been established between SMS and GCNet by the time this project is initiated.

## PT Infrastructure

### Provincial/Territorial Infrastructure Service Costs



Much like the Federal infrastructure service costs, each service that needs to be set up could cost \$500K. This is based on the development work to set up a service between ESDC's Social Insurance Register and IRCC's Global Case Management System.

It is assumed that each department/agency would have one application/solution that needs to have services added to. Further costs to connect internal applications have not been included.

Required Services to set up for Authoritative Parties	Cost for Service Development	Cost Model
Validation of Birth information from VSO	\$500K	Based on equivalent IT ESDC Development work (SIR → GCMS) ~500K per Service
Notification of Birth information from VSO	\$500K	
Notification of Death information from VSO	\$500K	
Validation of Driver's License information from SM	\$500K	
Validation of Health Information from SM	\$500K	
<b>5 Services</b>	<b>\$2.5M</b>	<b>~500K per Service</b>
<b>Multiplied by 13 PTs</b>	<b>\$32.5M</b>	

Required Services to set up for Relying Parties	Cost for Service Development	Cost Model
Validation of Birth information from VSO	\$500K	Based on equivalent IT ESDC Development work (SIR → GCMS) ~500K per Service
Validation of Immigration and Citizenship Information from IRCC	\$500K	
Notification of Death information from VSO	\$500K	
Validation of Driver's License information from SM	\$500K	
Validation of Health Information from SM	\$500K	
Validation of Social Insurance Number information from ESDC	\$500K	
Validation of Indian Status information from INAC	\$500K	
<b>7 Services</b>	<b>\$3.5M</b>	<b>~500K per Service</b>
<b>Multiplied by 13 P/Ts</b>	<b>\$45.5M</b>	

ELEMENTS	LOW	HIGH
Additional PT Infrastructure Development costs	TBD	TBD
<b>TOTAL – Technical Costs</b>	<b>Low = \$57.1M</b>	<b>High = \$114.2M</b>

\*\*\*While costs for relying party information exchange are a valid item for costing, it is believed that these costs will be covered by the respective department or jurisdiction needing that data. As such, they are not included in the final totals.

CDI Costing Overview		
Item	Low Estimate	High Estimate
<b>Federal Services Costs</b>		
Services - Authoritative Party (3 services anticipated)	\$1,500,000	\$3,000,000
Services - Relying Party <sup>§</sup> (6 services anticipated x 11 departments/agencies)	\$33,000,000	\$66,000,000
<b>Federal Infrastructure Costs</b>		
Hardware, Platform, Software <sup>*¥</sup>	\$3,400,000	\$6,800,000
<b>Central Infrastructure</b>		
Hardware, Platform, Software, Services, Connectivity <sup>¥</sup>	\$19,700,000	\$39,400,000
<b>PT Infrastructure Costs</b>		
Unknown	TBD	TBD
<b>PT Services Costs</b>		
Services - Relying Party <sup>§</sup> (7 services anticipated x 13 jurisdictions)	\$45,500,000	\$91,000,000
Services - Authoritative Party (5 services anticipated x 13 jurisdictions)	\$32,500,000	\$65,000,000
<b>Total</b>	<b>\$57,100,000<sup>ø</sup></b>	<b>\$114,200,000<sup>ø</sup></b>

\*No departmental modification costs are covered in this figure

¥ Add 20% for O&M

§ While costs for relying party information exchange are a valid item for costing, it is believed that these costs will be covered by the respective department/agency or jurisdiction needing that data. As such, they are not included in the final totals.

∅ Totals do not reflect relying party costs nor any business process costs