Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

AUDIT & COMPLIANCE REPORT F17-01

Insurance Corporation of British Columbia Information Sharing Agreements

Drew McArthur
Acting Information and Privacy Commissioner for British Columbia

September 13, 2017

CanLII Cite: 2016 BCIPC 39
Quicklaw Cite: [2016] B.C.I.P.C.D. No. 39

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

The Insurance Corporation of British Columbia (ICBC) maintains one of BC's most complete personal information data sets. Millions of BC residents are required to provide their personal information to ICBC to obtain a driver's licence, register or insure a vehicle, or process an insurance claim.

Data sharing is unavoidable in our economy. To access government programs, we must provide our personal information, and that information is collected, shared, used, and shared again, sometimes without our knowledge or consent. ICBC is authorized to share data with numerous public bodies and private organizations, from bailiff services and municipalities to parking lot operators and tow companies.

For these reasons, I selected ICBC for this special report, the fifth examination conducted by my Audit & Compliance team.

My auditors examined 94 information sharing agreements to confirm that ICBC fulfills its duty under the *Freedom of Information and Protection of Privacy Act* to protect the personal information of British Columbians. I was pleased overall with their findings. For the most part, disclosures of personal information by ICBC to approved third parties are reasonable and proportionate to its intended use.

That said, my auditors did find that ICBC could improve by tracking and reviewing third party access to personal information. ICBC should also conduct additional compliance monitoring of third parties as well as internal audits and reviews of ICBC systems, policies, and information sharing governance.

This report makes 12 important recommendations that will help ICBC maintain the trust of BC residents. These recommendations fall into three categories: Information Sharing Agreements, User Access Provisions, and Compliance Monitoring.

My office will follow up in three months to assess ICBC's progress toward implementing these recommendations.

ORIGINAL SIGNED BY

Drew McArthur
Acting Information and Privacy Commissioner for BC

EXECUTIVE SUMMARY

Under the authority of s. 42 of the *Freedom of Information and Protection of Privacy Act* (FIPPA), the Office of the Information and Privacy Commissioner (OIPC) conducted an audit of the Insurance Corporation of British Columbia's (ICBC) information sharing agreements (ISAs).

The Commissioner ordered this audit because numerous public bodies and private organizations can access the personal information ICBC collects from drivers, vehicle owners, insurance policy holders and other BC residents.

The scope of this audit includes:

1. Reviewing ICBC policies and practices on sharing and protecting the personal information of drivers, vehicle owners, and insurance policy holders;
2. Examining a sample of ICBC ISAs;
3. Analysing ICBC user lists to determine the third parties that have access to databases containing personal information;
4. Verifying ISAs where third parties have database access; and
5. Interviewing select ICBC staff.

OIPC auditors built assessment criteria and tools based on FIPPA obligations, OIPC guidance documents and orders, and ICBC's information sharing policies and procedures. This audit assesses whether ICBC:

- has an adequate policy framework relating to the approval, drafting, and monitoring of ISAs;
- has met its obligations under FIPPA, OIPC guidance documents and orders, and ICBC policies relating to the collection, use, disclosure, protection, and retention of personal information; and
- protects personal information as required by s. 30 of FIPPA.

ICBC collects information principally to issue driver licences, vehicle licences and registrations, insurance policies, and identification cards, as well as to process claims. ICBC discloses some of this information to certain municipal, provincial, and federal government bodies, law enforcement, and private sector organizations, such as parking lot operators, bailiff services, and tow companies.

Third parties may request an ISA with ICBC when they have numerous or ongoing requests for information sharing but must meet screening criteria before ICBC approves the ISA. If ICBC approves, the corporation discloses personal information to third parties either through direct means, by allowing third party users to access predetermined sets of data from their own

workstations, or through indirect means, whereby ICBC staff provide the information to third parties upon request.

Auditors reviewed all (24) direct access ISAs and a random sample of indirect access ISAs. Based on the review, auditors found that:

- ICBC has authority under FIPPA to disclose personal information for the purposes detailed in each of the ISAs.
- The disclosure of personal information is generally reasonable and proportionate for the intended use by third parties.
- The majority of ICBC's ISAs contain the essential components of what OIPC guidance documents state ISAs should contain.

Auditors found that ICBC could do more to safeguard personal information. This report offers 12 recommendations that will help ICBC comply with legislative obligations to protect personal information.

The recommendations include:

- amending ISAs, when they are up for renewal, to incorporate collection authority, rationale for disclosure, custody and control, breach management, training and notification to ICBC in the event of staff termination;
- tracking and reviewing third party access to personal information held by ICBC, removing duplicate and outdated userIDs, and ensuring that an ISA is in place before granting access to third parties; and
- conducting additional compliance monitoring with third parties as well as internal audits and reviews of ICBC systems, policies, and information sharing governance.

Commitment from ICBC executive is essential to providing adequate governance of ICBC's third party information sharing program.

1.0 INTRODUCTION

The Office of the Information and Privacy Commissioner for BC (OIPC) established the Audit & Compliance Program to assess how effectively public bodies and private sector organizations protect personal information and comply with access provisions under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

FIPPA governs the collection, use, and disclosure of personal information by public bodies. Under the authority of s. 42 of FIPPA, the OIPC conducted an audit of the Insurance Corporation of British Columbia's (ICBC) information sharing agreements (ISAs).

ICBC is a provincial Crown corporation that provides basic and optional auto insurance to BC motorists. ICBC also issues driver licences, vehicle licences and registration, and identification cards.[1] Through these services, ICBC collects and holds the personal information of millions of individuals who have driver licences, insurance policies, insurance claims, voluntary identification cards, and BC Services Cards.

The Commissioner ordered this audit because numerous public bodies and private organizations have access to personal information ICBC collects relating to drivers, vehicle owners, insurance policy holders and identification of BC residents. The audit examines four areas:

1. Third party information sharing request process
2. ISA contents
3. Use of access controls
4. Compliance monitoring of third parties

1.1 Objectives, scope, and methodology

This audit reviews ICBC's compliance with Part 3 of FIPPA, which covers collection, use, disclosure, protection, and retention of personal information by public bodies. The OIPC audit team developed the assessment criteria and tools based on FIPPA obligations, OIPC guidance documents and orders, and ICBC policies on information sharing and protection of personal information.

This audit has four objectives:

1. Review the extent to which ICBC processes and ISAs reflect legislative requirements;
2. Examine third party access to the personal information of drivers, vehicle owners, and insurance policy holders;
3. Identify any risk factors in the protection of personal information; and

4. Formulate recommendations to strengthen ICBC policy and practice.

The scope of this audit is limited to five components:

1. Reviewing ICBC policies and practices on sharing and protecting the personal information of drivers, vehicle owners, and insurance policy holders;
2. Examining a sample of ICBC ISAs;
3. Analysing ICBC user lists to determine the third parties that have access to databases containing personal information;
4. Verifying ISAs where third parties have database access; and
5. Interviewing select ICBC staff.

See Appendix A for more detail on the methodology.

2.0 LEGISLATION

2.1 Legislative background

The purposes of FIPPA are to make public bodies more accountable to the public and to protect personal privacy. Part 3 of FIPPA requires public bodies to appropriately access, collect, use, disclose, and dispose of personal information. ISAs explain the terms and conditions for sharing personal information between a public body and one or more third parties.

ICBC collects personal information directly from individuals under the authority of s. 26 of FIPPA. Sections 33 to 36 of FIPPA authorize ICBC, in certain circumstances, to share some personal information with other public bodies. Other provincial and federal statutes in conjunction with FIPPA may authorize or require certain third party agencies to indirectly collect personal information in ICBC's custody.

Public bodies that may indirectly collect personal information from ICBC include municipalities, law enforcement, provincial government bodies (e.g., to assist with collecting a debt owed to the government or to support a program), Elections BC, and Statistics Canada. ICBC also shares some personal information with private sector organizations, such as parking lot operators, towing companies, vehicle repair shops, financial institutions, and law firms.

2.2 Collection, use, and protection of personal information

2.2.1 Collection of personal information

ICBC collects personal information under s. 26(a) and (c) of FIPPA to enable its vehicle and driver licence programs and their related activities:

> 26 A public body may collect personal information only if
>
> (a) the collection of the information is expressly authorized under an Act, …
>
> (c) the information relates directly to and is necessary for a program or activity of the public body…

ICBC also collects personal information under the authority of the *Commercial Transport Act*, the *Motor Vehicle Act*, the *Insurance Vehicle Act*, and the *Insurance Corporation Act*.

2.2.2 Notification

Section 27 of FIPPA requires that, with limited exceptions, a public body explain the purpose for collecting the information and the legal authority for collecting it. The public body must also provide contact information for an individual who can answer any questions about the information collection.

2.2.3 Accuracy and correction

As is commonly found in privacy legislation, ss. 28 and 29 of FIPPA require that public bodies make reasonable efforts to ensure the accuracy of the personal information under its custody and control. FIPPA also gives an individual a right to correct his or her personal information.

2.2.4 Protection of personal information

In accordance with s. 30 of FIPPA, public bodies must take reasonable precautions to protect the security of personal information under their control with organizational, physical, and technological safeguards.

2.2.5 Storage and access must be in Canada

Section 30.1 of FIPPA requires that public bodies ensure they store and access personal information in Canada unless the individual has consented or FIPPA permits disclosure outside of Canada.

2.2.6 Use of personal information provisions

Section 32 of FIPPA limits how public bodies can use personal information in their custody or under their control. They may only use personal information for the purposes it was collected or for a use consistent with that purpose. They may only use the information for a different use if they have consent from the individual.

2.3 Disclosure of personal information

Section 33 of FIPPA permits a public body to disclose personal information in its custody or under its control only in specific circumstances. Sections 33.1 and 33.2 provide specific considerations for disclosure inside or outside Canada and for disclosure inside Canada only.

Section 33.1(1) permits disclosure *inside or outside* Canada when, for example:

- the individual has consented;
- another enactment permits disclosure;
- disclosure is for collecting amounts owing or payment to the government of British Columbia or a public body; or
- disclosure is for licensing or registering licenses or registrations of motor vehicles or drivers, or verifying vehicle insurance, registrations, or driver licences.

Section 33.1(4) also permits ICBC to disclose personal information obtained or compiled for insurance purposes if disclosure is necessary to investigate, manage, or settle a specific insurance claim.

Section 33.2 of FIPPA limits disclosure to *inside Canada* when, for example:

- use of the personal information is consistent with the purpose for which the information was obtained;
- the information is necessary for the protection of the health or safety of an officer, employee, or minister of a public body;
- the information is shared with the auditor general or any other prescribed person or body for audit purposes; and
- the information is shared with a public body or law enforcement agency to assist in a specific investigation where a law enforcement proceeding is likely to result.

Section 34 of FIPPA clarifies the criteria for determining whether the use of personal information is consistent with the original purpose: the use must have a reasonable and direct connection to that purpose and the information must be necessary for performing statutory duties or for operating a program or activity.

2.4 The Information Sharing Agreement

Public bodies or private organizations commonly use ISAs to regularly exchange information. Section 69 of FIPPA defines an ISA as an agreement between a public body and another entity or person that describes conditions on collection, use, or disclosure of personal information by the parties to the agreement.

Information sharing may involve one party disclosing information and the other party receiving or collecting it. It can also refer to an exchange of information, where both parties disclose and collect information. A Memorandum of Understanding that addresses personal information sharing may also qualify as an ISA.

Public bodies and organizations should document the terms and conditions before sharing personal information.

2.4.1 ISA administration

Legislation can prescribe the contents of an ISA[2] FIPPA also requires ministries to prepare ISAs in accordance with directions of the minister responsible for the Act. At the time of writing this report, the minister has not issued such direction to ministries.

To meet legislated obligations, public bodies and organizations should share the least amount of personal information necessary to fulfil the intended purpose and must have appropriate safeguards to protect the personal information pursuant to s. 30 of FIPPA and s. 34 of PIPA. Public bodies and organizations can help protect personal information by communicating expected safeguards to third parties within a written ISA. Generally, senior individuals who have authority to act for the public body or organization sign ISAs.

An example of existing guidance on ISAs is the OIPC's *Physicians Toolkit*. This guideline is useful for public bodies or organizations sharing personal information with third parties on a routine and regular basis. These guidelines state:

> An ISA will usually:
>
> - Reference all applicable legislation that provides the legal authority for collection, use, and disclosure of personal information.
>
> - Identify
> - types of information that each party will share with each other
> - the purpose for data sharing
> - permitted uses for the specified purpose
> - disclosure restrictions
> - retention periods
> - who has custody and control of the information
>
> - Describe
> - what personal information will be shared
> - who will have access and under what conditions
> - how personal information will be exchanged
> - security safeguards in place to protect information
> - secure destruction methods when retention expires
> - processes for:
> - responding to access requests by individuals whom the personal information is about
> - ensuring accuracy
> - managing privacy breaches, complaints, and incidents
> - terminating the agreement.[3]

3.0 OVERVIEW OF ICBC PROCESS

The President of ICBC, as head of the public body, is responsible for decisions about collection, use, and disclosure of the personal information. The Chief Legal Officer has operational responsibility for privacy functions. In practice, the Privacy and Freedom of Information (PFOI) Manager develops information sharing policies and procedures. Senior staff in each business unit of ICBC also share responsibility for implementing policies and procedures.

This section outlines ICBC's policies and processes for collecting and disclosing personal information, the steps for reviewing and approving information sharing requests, the security safeguards in place to protect personal information, and ICBC's recent review of their information sharing program.

3.1 Notification for collection and disclosure

ICBC's privacy policy states that ICBC will only collect personal information directly from customers, unless it has specific authority to do otherwise, and it will not disclose personal information to anyone without consent or statutory authority. The policy also requires staff to explain why ICBC collects personal information.[4]

ICBC collects information principally to issue driver licences, vehicle licences and registrations, insurance policies, and identification cards and to process claims. ICBC informs the public about its collection and disclosure of personal information on driver licence application and renewal forms, owners' certificates of insurance, on its website, and on signage within some driver licensing centres.

The driver licence application and renewal forms state:

> ICBC collects personal information under the authority of section (s.) 25 or s. 31 of the Motor Vehicle Act and s. 26 of the Freedom of Information and Protection of Privacy Act ("FIPPA") for the purpose of processing your application for a BC Driver's Licence and Service Card, its authorized programs and your enrolment in the Medical Services Plan. Information may be disclosed pursuant to section 33 or 81 of FIPPA.[5]

The owners' certificate of insurance and vehicle licence states:

> ICBC may use or disclose this information in accordance with provisions of the Freedom of Information and Protection of Privacy Act and may disclose this information, along with your claims history, to an insurer in another province if you apply for insurance outside of British Columbia.[6]

ICBC provides general notification about disclosure of personal information on its website:

> "There are some circumstances where we may disclose or share some personal information about you. These circumstances are mainly for purposes consistent with the reasons we collected the information in the first place, such as the use of your personal information in renewing your insurance policy. Other examples are:
>
> - To comply with requests from law enforcement agencies; for example, disclosing an owner's information to police when a stolen vehicle is found.
> - To meet legal requirements during a court proceeding or regulatory requirements such as those associated with providing information to RoadSafetyBC.[7]
> - To update the voter registration list as required by the Elections Act.
> - To assist in collecting a debt owed to ICBC or another public body as permitted by FIPPA."[8]

3.2 Disclosure policies and processes

ICBC discloses customers' personal information to certain municipal, provincial, and federal government bodies, law enforcement, and private sector organizations, such as parking lot operators, bailiff services, and tow companies. Third parties may request an ICBC ISA when they have numerous or ongoing requests for information sharing.

Third parties must meet screening criteria before ICBC approves an ISA. PFOI staff initially review requests from third parties to determine whether a legal authority exists to share the requested information.[9] If PFOI staff believe statutory authority exists and that the request is reasonable, they forward the request to ICBC's Access Information Review (AIR) Committee for consideration.

The purpose of the AIR Committee is to "review requests for access to personal information in ICBC's custody as set out herein, and to make decisions as to whether such access should be granted."[10] The AIR Committee has an advisory role and approval authority, delegated by the Head of the Public Body.[11] AIR Committee decisions are final, with no appeal process for third parties.[12]

In the past, the AIR Committee met three or four times annually to review ISA requests. Due to fewer requests for ISAs, the AIR Committee now meets on an as-needed basis. Requests for ISAs have varied from a high of 11 in 2012 and 2014 to a low of one request in 2016.[13] There are presently 247 active ISAs between ICBC and third parties.

According to the AIR Committee's *Guidelines for Review of Direct Access Agreements*, the Committee bases their decision on a Privacy Impact Assessment or an Access to Information Questionnaire submitted by the third party. With this information, the AIR Committee:

- reviews the legal authority under which the third party is requesting access;

- determines the business reasons for the third party collection and use of the personal information;
- determines the specific personal information involved; and
- decides whether to grant the disclosure and the method by which disclosure would occur.[14]

In addition to the AIR Committee, ICBC's Driver Testing and Vehicle Information (DTVI) unit directly decides certain common requests for access (for example, from municipalities), provided the application is not unusual.[15]

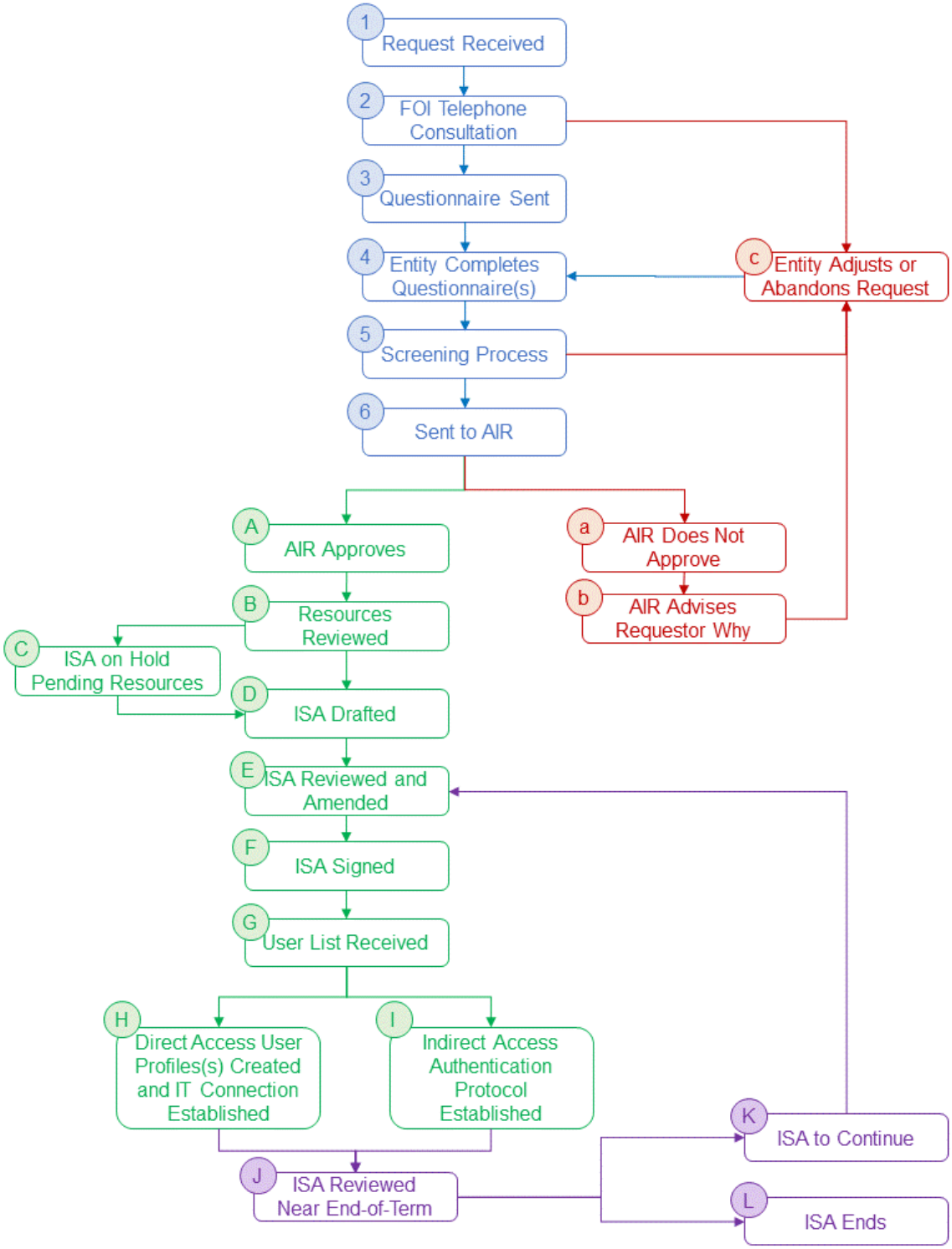
Once ICBC approves an ISA request, it determines the systems and data elements it will make available to the third party and the number of individuals who require access.[16] ICBC then drafts the ISA, which details policies and processes. Both parties review and sign the ISA, and then the information sharing can begin.

ICBC discloses personal information to third parties through one of two methods:[17]

- **Indirect access**: Third parties submit requests by telephone, fax, or email to ICBC through its Contact Centres (primarily to the DTVI department). ICBC staff look up the information for the third parties and respond back via telephone or electronically.
- **Direct access**: Third parties log into ICBC systems from their own workstations and directly access predetermined sets of personal information data.

Figure 1 provides a detailed depiction of ICBC's ISA Approval Process.

Figure 1: ISA Approval Process



3.2.1 Indirect access

ICBC does not grant direct access to their databases to private organizations (for example, parking companies, bailiff services, towing or vehicle repair) or municipal governments. Instead, these third parties submit requests to ICBC by phone, fax, email, mail, or secure file transfer protocol. The requestor provides ICBC with a vehicle identification number, licence plate number, claim number, and/or name and ICBC discloses personal information such as licensing information, vehicle descriptions, and/or registered owner names and addresses.

DTVI staff generally respond to these requests by phone or electronically.[18] Call centre staff follow ICBC processes and guidance to authenticate the requests prior to disclosure.[19] ICBC provides staff with procedural guidance through the DTVI Reference Manual[20] and Verification Procedure.[21]

3.2.2 Direct access

Some provincial government bodies and law enforcement agencies have ISAs that allow direct access to ICBC databases. Employees of these third parties individually log into ICBC systems (either via provincial government computer system or, for law enforcement, through the Canadian Police Information Centre (CPIC) network) and access previously specified sets of ICBC customer personal information.[22]

The personal information shared through direct access can be more sensitive and may include, for example, name changes, physical descriptions of individuals (such as height, weight, hair colour, and eye colour), claims information, violation ticket information, and/or driving contraventions. Due to the sensitivity of the information, third party staff with access to such information are subject to additional electronic verification procedures.

ICBC provides direct access to personal information through access profiles that reflect the "need to know" principle, limiting information to only what is required.[23] ICBC provides new users with access profiles consistent with ministry-specific profile charts and mirrors new user profiles using an existing profile from the relevant chart.[24] After creating an access profile, ICBC sends a userID to the third party. Users then create their own passwords and are able to access the system through the direct connection, where they can view only the personal information allocated to their specific profile.

In some cases, ICBC is unable to provide direct access due to technical limitations. In these situations, applicants obtain a userID from the provincial government's shared IT services to gain access through the Shared Provincial Access Network/BC (SPAN BC).[25]

3.4 Security safeguards

According to ICBC's policy, "Protecting the Privacy of Personal Information," ICBC:

> …take[s] all reasonable measures to protect the security of personal information" and has put in place various safeguards including:
>
> - Physically, by building security and physical barriers;
> - Organizationally, by policies, procedures and access level controls; and
> - Technologically, by such means as use of passwords, encryption, firewalls, and anti-virus software and data monitoring.[26]

3.4.1 Physical safeguards

ICBC employs security guards at both entrances to its headquarters and access cards are necessary to enter working areas of the building. Visitors must sign in and ICBC staff escort them while they are inside the building.

ICBC servers store the electronic data it collects, including the personal information of its customers, which is located at a separate data centre. According to ICBC's Manager of Information Risk Management, the data centre has multiple check-in points and secured gates, with different servers in different secure cages, and data centre staff only allow individuals to enter the facility if they have an operational need (for example, maintenance technicians).

3.4.2 Organizational and administrative safeguards

ICBC has an array of privacy and security policies, standards, and guidelines that explain and inform staff of the organization's privacy and security requirements.

The purpose of the Protecting the Privacy of Personal Information policy is to "assist ICBC employees, contractors, brokers, and other business partners in understanding the principles that underlie our privacy commitments, and to understand their role in protecting personal information."[27]

For security purposes, ICBC has an Enterprise Information Management department and a Data Governance department. Supporting these departments is an information security program to "ensure reasonable controls are in place to protect against the unauthorized alteration, destruction, and disclosure of personal and corporate information."[28]

The Information Systems Security policy is ICBC's primary security policy. ICBC also has a "Technical Vulnerability Standard" that states that ICBC will develop a technical vulnerability management program to effectively manage the information security risk exposure to ICBC systems and data.[29]

Privacy breach requirements for ICBC and third parties

In their Privacy Breach Guidelines,[30] ICBC provides specific guidance to staff on how to identify and manage privacy breaches. In addition, ICBC's Information Systems Security policy states that "users found to be inappropriately accessing or using ICBC information systems are subject to disciplinary action up to and including termination of employment."[31]

While the above guidance applies only to ICBC staff, the Security Incident and Violation Reporting Standard applies to "all employees and external parties who use ICBC systems and services."[32] This Standard requires employees and managers "to report all security incidents, events, and violations, whether they are intentional or accidental."[33] However, the Standard does not address accountabilities, reporting process, or requirements when security incidents or third-party breaches occur.

In 2014, ICBC's Corporate Audit Services reviewed the three privacy breaches that third parties reported in the 18 months ending June 30, 2014. They found that the ISA template's wording on breach reporting was adequate in communicating requirements and expectations for reporting privacy breaches to ICBC.[34]

Other safeguards

Other organizational and administrative safeguards affect technological security. These include:

- a log of all user access to ICBC systems;
- a Privileged Access Security Standard;[35]
- rules for use and management of removable media;
- rules for exemptions from the Information Systems Security policy; and
- requirements that the Information Risk Management department review its policies annually, hire a third party to review its Information Security Policy, and create a new strategy every four years.[36]

3.4.3 Technological safeguards

The Chief Information and Technology Officer is accountable for the Information Security Program policy and the Information Risk Management department manages the Information Security Program and develops and maintains the policy.[37]

Under ICBC's Information Systems Security policy, ISAs should specify when information is in ICBC's custody and responsibility and when that custody and responsibility transfers to or from a third party.[38] The security policy states:

> All remote access solutions accessing the ICBC network must ensure that appropriate security protections are in place between the corporation's network and public networks

> or networks owned by other organizations. Authentication mechanisms for remote access solutions must have protection levels equal to the risk of the environment the user is operating in.[39]

During an interview, ICBC staff explained the comprehensive security program used to manage direct electronic access by third parties.

ICBC uses a secure file transfer protocol for third parties with indirect access to mitigate the risk of interception of information.

Third parties with direct access log in to ICBC's databases through Citrix or SPAN BC that connects their government workstations to ICBC's Multiple Virtual Storage system. Third party employees are able to copy, paste, and print the information available to them.

ICBC staff reported that security controls include userIDs, passwords, multi-factor identification for users with remote access, and role-based access privileges specific to authorized employees, their role, and the function of the third party.

ICBC staff also described multiple layers of control. These include traditional controls for connecting to the internet such as firewalls, email gateways, web-browser gateways, other gateways, and end-point security to block malicious traffic from its internal network.

ICBC's policy on information asset identification and classification requires ICBC to authenticate all users before granting them access to ICBC systems. [40] This policy, and the Password Creation and Management Standard, also provide rules for:

- standardized password creation and management;
- prohibitions against writing down or sharing passwords; and
- changing passwords whenever there is a risk that they are no longer secure.

Most of these rules apply only to ICBC staff and not to third party users of ICBC systems. The Standard also encourages users to change their passwords at least once every 180 days.[41] Processes are also in place to remove inactive userIDs after 90 days.[42]

In summary, ICBC has Application Design and Information Security Standards that, along with the Information Systems Security policy, require that all ICBC systems are developed, configured, customized, and maintained for protection from any internal or external threats.[43]

3.5 Compliance, governance and accountability

In 2013, ICBC completed a Privacy Compliance Review.[44] The reviewers deemed "third party data governance" to be high risk and identified four key issues:

- Insufficient compliance reviews and lack of enforcement and monitoring of ISAs;
- Insufficient clarity around roles and responsibilities when reviewing third party ISAs for compliance;
- Inconsistent or no training of third parties, and no review of third parties' privacy training programs; and
- Inconsistent notification to business areas any changes if agreements with third parties are cancelled or modified.[45]

In 2014, ICBC's Corporate Audit Services specifically examined governance of providing personal information to third party agencies. The auditors found that the controls to support governance of third party information sharing were only partially effective, the governance framework was incomplete, and a corporate policy was necessary.[46]

In response to these findings, management stated that the PFOI department would, by end of Q1 2015, complete outstanding work in the following areas:

- Revise the Disclosure to Other Agencies policy,
- Negotiate outstanding ISAs,
- Design and implement the Third-Party Compliance Review program,
- Work with DTVI to streamline the process for collecting third party authorized employee lists,
- Implement the new monitoring program over providing information to law enforcement agencies, and
- Work with Access and Security Operations (ASOps) and Information Services Department's Solutions Sustainment team to document and develop access profiles for direct access users and update the Ministry Profile Chart (by the end of Q2 2015).[47]

In 2015, ICBC initiated the "Third Party Compliance Review (TCR) Program" aimed at preventing a significant privacy breach involving ICBC personal information.[48] Activities in the TCR Program include:

- questionnaires for self-reported compliance reviews;
- site visits to high-risk locations to inspect records, facilities, and computers;
- transactions and records audits involving third party user logins or information requests;
- volume audits of user access by those with numerous logins over a defined period;
- review of electronic reports such as access logs for specified parties;
- review of third parties with many users who do not login for over 90 days (userIDs that have not been used for 90 days are automatically deleted); and
- audits of third party information practices.

For third parties with indirect access, ICBC sent compliance review questionnaires. ICBC then ranked these organizations based on risk level (determined by the volume of information, sensitivity of information, number of users, and recipient profile).[49] It provided recommendations in writing to medium-risk locations, and conducted site visits to all locations identified as high risk. However, ICBC has not conducted compliance monitoring of third parties who have direct access. It plans to conduct this monitoring in 2018.

4.0 FINDINGS

In total, OIPC auditors reviewed a random sample of 94 ISAs. This section summarizes the findings and:

- outlines ICBC's disclosures through ISAs;
- examines the detail and contents of the ISA documents;
- evaluates compliance with FIPPA, OIPC guidance, and ICBC policies;
- summarizes ICBC's access controls; and
- discusses ICBC's governance of third party information sharing.

4.1 Disclosure of personal information

4.1.1 Parties to the agreements

ICBC does not grant access to every public body or organization that requests access to the personal information. ICBC has an extensive review and approval process for considering new ISAs, which the OIPC deems adequate.

ICBC discloses personal information predominantly to public bodies, which constitute 72% of its 247 ISAs. Most ISAs (47%) are with municipalities. Other public bodies with ISAs include police and provincial government ministries (11% and 10%, respectively), other government agencies (for example, Statistics Canada or Canadian Border Services Agency, 4%) and tolling companies (1%). With larger public bodies, such as the provincial government, ISAs exist with specific ministries and departments.

The remaining 28% of ISAs are with private sector organizations. Law firms and parking companies comprise the largest groups of private sector ISAs (9% and 8%, respectively), while other organizations such as court bailiffs, vehicle repairers, towing companies, financial institutions, and registry companies comprise one to 3%.

4.1.2 Categories of personal information shared

Third parties with approved ISAs access or receive different categories of personal information based on the purpose for information sharing:

1. **Municipalities** indirectly receive contact details, insurance coverage expiry information, and vehicle identifiers.
2. **Police and law enforcement** (external to BC) directly access contact details, personal identifiers, driver licence information, insurance coverage information, and vehicle identifiers.
3. **Other government agencies,** such as Statistics Canada and Transportation Investment Corporation, directly access contact details, personal identifiers, digital images, law enforcement information, driver licence information, insurance coverage information, and vehicle identifiers.
4. **Provincial government bodies** directly access all of the above personal identifiers plus account/security keyword, debt information, vehicle financial information, employment information, business relationship/partnership information, surplus information, and ICBC damaged vehicle history.
5. **Law firms, parking companies, towing companies, vehicle repairers, BC registries, and court bailiffs** indirectly receive contact details, insurance expiry information, and vehicle identifiers.
6. **Financial institutions** indirectly receive vehicle identifiers.
7. **Tolling companies** indirectly receive contact details, insurance coverage details, and vehicle identifiers.

ICBC also shares personal information with police agencies without an ISA, as well as with some public bodies and private sector organizations using other types of agreements that contain provisions governing the protection of personal information. These include provincial government Service BC agents who provide ICBC services in remote communities and private vehicle insurance brokers who manage insurance sales on behalf of ICBC.

Based on the sample of ISAs, the most common personal information that ICBC shares with third parties includes basic contact details (98%) and vehicle identifiers (95%).

In general, parties with direct access receive more sensitive personal information and parties with indirect access receive less or non-sensitive information.

Based on the sample, the most sensitive information shared with third parties includes:

- **Personal identifiers** (36% of the sample, comprised of provincial government, CPIC agencies, the Medical Services Commission, and the Canadian Council of Motor Transport Administrators or CCMTA;
- **Law enforcement information** (9% of the sample, provincial government agencies and CCMTA);
- **Security keyword** (9%, only provincial government agencies); and

- **Digital images** (3%, BC Ministry of Finance and the CCMTA).

Table 1 provides detail on the categories of personal information ICBC discloses.

Table 1: Categories of Personal Information ICBC Discloses	% of ISA
Contact details: Name, address, postal code, previous address and name, address effective and termination dates, customer service number, telephone number	98%
Vehicle identifiers: Vehicle identification number (VIN), vehicle plate and client numbers; air endorsement indicator; vehicle colour, body, make, model, weight, purchase history, and licence plate history	95%
Insurance coverage and expiry: Policy registration status, exemption codes and history	77%
Driver licence information: Driver licence number, BC Identification number, status, history, and out-of-province driver licence number	36%
Personal identifiers: Gender, date of birth and death, personal health number, height, weight, hair colour, eye colour	36%
Financial: Vehicle lease and auto plan payment, pro-rate, and financial responsibility	13%
Surplus information: Personal information that the third party can view but is not required for third party use	10%
Law enforcement: Driving contraventions, prohibitions, suspensions, police file number, specific information on suspects, violation ticket number, and enforcement officer's name	9%
Account/security keyword: A word ICBC customers provide to verify their identity	9%
Claims: Claim number, status, history and jurisdiction; percent liability, date of loss, and loss location	6%
Digital images: Driver licence photograph	3%
Debts: Fine amount, payment date	3%
Business: Business relationship and business partner information	3%

"Surplus information" is additional personal information that third parties can view, even though they may not need it. This personal information is not necessary for the program or activity of the third party, so collecting it does not meet the provisions of FIPPA s. 26(c).

Therefore, FIPPA does not authorize third parties to collect or use this information and, by default, does not permit ICBC to disclose it under ss. 33.1 or 33.2.

This information is visible because ICBC provides access to certain screens with set fields of information that they say they have been unable to change due to the age and complexity of ICBC's driver licensing IT systems. Sometimes this information includes sensitive personal information, such as an individual's security keyword.

OIPC auditors raised the issue of unauthorized disclosure with ICBC. The PFOI manager reported that ICBC continues to review all of its direct systems access with ministries with the goal of more precisely matching the information required by each ministry with available screens.

RECOMMENDATION 1

ICBC should prevent unauthorized disclosure of personal information to direct access third parties.

4.1.3 Length of ISA terms

Of the 247 ISAs ICBC manages:

- One percent expire within one year of the date of signing;
- 64% expire within three years;
- 28% expire within five years;
- Two percent expire within eight years; and
- Four percent have no expiry date (mostly other government offices, such as Statistics Canada).

OIPC auditors could not determine the terms of three ISAs. Two of these were still in draft form during the review.

According to ICBC, for indirect access ISAs, DTVI flags ISAs due for renewal. Third parties submit a renewal questionnaire that includes the purposes for collection and confirmation that they have an information handling policy that details collection, use, disclosure, security, retention and disposal policies as well as how to manage complaints. ICBC reviews the questionnaire and decides whether continued information sharing is warranted.

ICBC is currently drafting policy and procedures for managing renewals of direct access ISAs. Most of these ISAs are for three years and will be up for renewal in 2017.

4.2 Content of ISAs

OIPC auditors reviewed the sample of ISAs against 73 data points and found that the majority contain the essential components outlined in the OIPC's *Physicians Toolkit*.[50] This section follows the basic order of items as listed in that guidance document.

4.2.1 Legal authority

All ISAs in the sample list the authority under FIPPA for ICBC's disclosure of personal information. Eight of the ISAs (mostly with private sector law firms) refer to disclosure under s. 33.1(1)(j), which government repealed in 2011.

Only 29% of the sample of ISAs list legislative authority for third party collection of the personal information. This made it difficult in some cases for OIPC auditors to determine whether or not FIPPA authorizes the disclosure. OIPC auditors raised seven ISAs for discussion with ICBC, as the third party's authorization for collection was not plain and obvious.

RECOMMENDATION 2

ICBC should include the following details in all ISAs:

a) The legal authority for third party collection of personal information.

4.2.2 Purposes for sharing

All ISAs in the sample detail the types of personal information ICBC shares with third parties and the permitted use of that personal information. OIPC auditors found the disclosure of personal information, as documented in the sample of ISAs, to be authorized and reasonable or appropriate for the intended use.

In most cases, it was plain and obvious how each specific category of personal information met the stated purpose. In other cases, it was less obvious. Less than one-quarter (23%) of the ISAs explicitly detail the purpose for *each* different category of personal information.

One instance where ICBC explicitly details the purpose for each different category of personal information is an agreement with the Ministry of Finance. In this ISA, the first categories of personal information are driver contact information and personal identifiers (i.e., name, address, date of birth) and vehicle identifiers (i.e., vehicle description, licence plate number, plate history, and policy details). The ISA specifically states that these types of information are necessary to verify ownership and timing of vehicle transfer and to verify additions or disposition of assets. The next set of personal information is physical descriptors of the

registered owner of the vehicle (i.e., height, weight, hair colour) and the stated purpose is to confirm an individual's identity during surveillance operations or investigations of tax fraud.

For transparency, where it is not plain and obvious, ICBC should explicitly state how sharing each specific category of personal information assists in achieving the purposes for disclosure.

RECOMMENDATION 2 (continued)

ICBC should include the following details in all ISAs:

b) The rationale for disclosure of each category of personal information, if it is not plain and obvious how the third party is entitled to collect or use the information.

4.2.3 Limitations on use

Within the sample, the most common uses of personal information by third parties are:

- law enforcement (51%);
- debt collection (46%);
- verification of details provided to government agencies or vehicle ownership information provided to private sector organizations (11%);
- management of insurance claims (11%);
- assistance in locating individuals (9%); and
- provision of payment to individuals (2%).[51]

Two ISAs contain vague wording for specified restrictions on use. For example, one statement includes "to allow its Authorized Employees to exercise the powers given to them and perform their duties under the [legislation]."

4.2.4 Access & disclosure

Nearly every ISA in the sample (99%) contains restrictions on who from the third party may access the personal information and to whom they can further disclose that information. In most cases, the individuals with whom third parties can further disclose personal information include:

- authorized employees;
- the third party's compliance representative;
- the individual whom the personal information is about;
- OIPC; and

- law enforcement.

Some ISAs include other external parties, such as auditors, collections agencies, and service providers. Where applicable, if the ISA permits disclosure by the third party to other parties, the third party must consider whether the information sharing is permissible under FIPPA and whether that disclosure required another ISA. In some cases, the ISA includes a requirement to provide ICBC with a copy of that ISA.

ICBC also sets restrictions, in accordance with FIPPA, on foreign storage and disclosure (evidenced in 98% of the sample of ISAs). Only the ISAs with the CCMTA and CPIC do not include such restrictions. These parties have the legal authority to disclose in foreign jurisdictions.

4.2.5 Information exchange

All of the ISAs in the sample mention the mode for information sharing (direct, indirect or combination of both), frequency, and the method for gaining access.

Within the sample of 94 ISAs, 60 provide indirect access to personal information (i.e., an ICBC employee looks up the information and provides it to the third party), while 30 ISAs provide direct access (i.e., third party employees look up the information themselves). The remaining four agencies have access both directly and indirectly.

ICBC provides direct access to third parties by creating system profiles reflecting the categories of personal information in the ISA. When the user signs into ICBC system, they only see the screens containing the pre-set personal information.

ISA provisions for indirect access require third party employees to provide basic information (such as an individual's name, a vehicle identification or plate number, or an insurance claim number), and confirm that they are an authorized user, before ICBC provides them with the personal information requested.

4.2.6 Custody and control

Only 2% of the sampled ISAs explicitly stipulate which party to the agreement has custody and control over the personal information they share. The ISA with the Medical Services Commission states:

> "All Personal Information shall be and remain in complete control of the disclosing party. No access to or custody of Personal Information by the receiving party… shall be construed in any manner as providing control or any other rights with respect to such Personal Information except as otherwise provided in this Agreement" (paragraph 6.6, page 5).

Establishing custody and control is necessary to determine who is responsible for safeguarding personal information in accordance with FIPPA and PIPA. ICBC's Information Systems Security policy states, "ISAs will specify when the security of information becomes ICBC's responsibility, and at what point it is no longer ICBC's responsibility to secure the information (in other words, when they transfer custody to/from the 3rd party)."[52] However, OIPC auditors found that ISAs do not clarify when third parties become responsible for securing personal information.

RECOMMENDATION 2 (continued)

ICBC should include the following details in all ISAs:

c) Identification of who has custody and control of personal information and at what point the custody or control changes.

4.2.7 Retention periods

ICBC reported that it keeps records in the driver licensing system in perpetuity. In the sample of ISAs, nearly all (98%) include ICBC's expectations on third party retention of records.

Seventy-one percent (71%) of the ISAs that contain retention requirements – comprised mostly of indirect access ISAs – require third parties to retain:

- records that reasonably establish the third party's need for each item of personal information for at least three years following the release of the information;
- audit logs for the term of the agreement plus two years; and
- the personal information itself for the required statutory period.

Another 18% of ISAs – comprised solely of direct access agreements – require third parties to hold records that establish the need for personal information for the term of the ISA, plus two years, and to hold audit logs for two years. A smaller number (7%) of direct access ISAs require third parties to retain records that establish their need for personal information for a period of two years.

Two ISAs (with CCMTA and CPIC) do not contain any retention provisions.

Though retention requirements varied considerably across the sample ISAs, OIPC auditors found the set retention periods to be reasonable.

4.2.8 Destruction methods

Nearly all (99%, all except CPIC) of the sample of ISAs contain requirements for secure destruction of records. Typical destruction methods include:

> Once personal information is no longer required, User will permanently and securely destroy the personal information and all records thereof in a manner that is appropriate for the media, so that the personal information or any portion of it cannot be subsequently retrieved, accessed or used by the third party or any other person.

4.2.9 Accuracy

Accuracy of the personal information held by ICBC varies. ICBC reported that individuals generally keep their driver licence addresses up-to-date, as required by law. If Canada Post returns mail as undelivered, ICBC flags the intended recipients address and notes that it is no longer valid.

Within the sampled ISAs, 97% contain provisions requiring third parties to respond to requests by individuals to correct their personal information if it is incorrect or incomplete. The ISAs require third parties to verify the accuracy of the personal information with ICBC and, where appropriate, advise the individual to make a formal request to ICBC for correction.

One-quarter of the sample of ISAs, comprising only direct access, also require the third party to advise ICBC that they have made a correction.

4.2.10 Managing incidents, complaints & breaches

Nearly all (96%) of the sampled ISAs require third parties to notify ICBC immediately of any anticipated or actual non-compliance with the ISA and to inform ICBC of steps taken to address the issue and prevent recurrence. The four ISAs that do not contain this requirement include:

- Transportation Investment Corporation;
- CCMTA;
- Canada Border Services Agency; and
- CPIC.

Seventy percent of the ISAs require third parties to have written procedures to resolve complaints. While the majority of ISAs with provincial and federal government agencies do not include complaint provisions, third parties may still have complaint processes already in place.

ISAs governing indirect access or access through the CPIC network require that third parties:

- have procedures to deal with complaints;
- provide a copy of the complaint to ICBC;
- document each complaint and its resolution;
- retain records and provide such to ICBC upon request; and
- respond to complaints in a timely manner.

OIPC auditors found that less than one-third (31%) of the sample of ISAs specifically require third parties to have a process for managing breaches. Of the ISAs that contain breach requirements (mostly direct access ISAs with provincial and federal government agencies), all require third parties to report breaches to ICBC. None of the ISAs with private sector organizations requires breach management or a requirement to report breaches to ICBC.

RECOMMENDATION 2 (continued)

ICBC should include the following details in all ISAs:

d) A requirement for third parties to have processes for managing and reporting breaches.

e) A requirement for third parties to have written procedures to resolve complaints about their information-handling practices.

4.2.11 Privacy policy & training

Two-thirds (64%) of the sampled ISAs require third parties to have information handling and privacy policies. OIPC auditors found that ICBC recently included this requirement in nearly all ISAs. The majority (91%) drafted prior to 2015 did not contain privacy policy requirements. In contrast, nearly all (97%) ISAs drafted since then include this provision.

Regarding training, 92% of direct access ISAs require that authorized staff "complete privacy training and an annual re-affirmation of their undertaking of privacy practices and protocols to comply with policy." Only two ISAs require that staff sign the undertaking *prior* to accessing to ICBC databases. In contrast, indirect access ISAs do not require third parties to train staff, with one exception: the ISA with Statistics Canada includes a provision for signing an undertaking.

RECOMMENDATION 2 (continued)

ICBC should include the following details in all ISAs:

f) A requirement for third parties to have a written privacy policy.

g) A requirement for third parties to provide privacy and security training to staff prior to gaining access to personal information collected by ICBC.

4.2.12 Physical & technological security

All ISAs include physical or technological security requirements. ISAs require third parties to "have appropriate physical, organizational and technological security measures in place to ensure that any and all personal information which is collected, accessed, used, disclosed or destroyed pursuant to this agreement is done so only by authorized employees."

In addition, ISAs include the following specific provisions:

- **Physical security:** Nearly every ISA (99%) in the sample explicitly require physical security for all personal information (the only exception was the ISA with CPIC).
- **Electronic storage:** ISAs restrict which employees may access electronic records and storage devices containing personal information. However, none of the ISAs require encryption of storage devices.
- **User access logs:** Most of the sample of ISAs (96%) stipulate that third parties must keep a log of who has had access to electronic records.
- **Unique userIDs:** Three quarters (72%) require third parties to provide each authorized employee with their own userID. In other cases, ICBC provides the employees with their own unique userIDs.
- **Updated employee lists:** Most ISAs (89%) require third parties to provide ICBC with an updated employee list. Exceptions are Statistics Canada, the CCMTA, and police agencies that access ICBC databases through CPIC.

4.2.13 Compliance monitoring

Nearly every (98%) sampled ISA requires third parties to designate a representative responsible for ensuring privacy and ISA compliance. The two ISAs that do not include this provision are CPIC and the CCMTA. The CPIC ISA (along with three other ISAs, or 4% of the sample) contains a clause addressing issues management and identifies the individuals responsible for resolving disputes about the agreement.

Every ISA in the sample contains at least some or all of the stipulations below:

- Third parties will provide ICBC with immediate written notification of any anticipated or actual non-compliance with the ISA and steps taken to address the issue and to prevent recurrence;
- ICBC may request a compliance review of the third party's information management policies and practices (including a review of user access logs, transactions, reports or other documents);
- ICBC may enter third party premises to inspect – when relevant to the third party's compliance with the ISA – any personal information in the custody of the third party and any information management policies or practices;

- Third parties will provide ICBC with an annual written certificate (i.e., a letter) confirming compliance with all obligations under the ISA; and
- An external auditor may be appointed to review the third party's information practices and the results shall be provided to ICBC.

OIPC auditors identified certain weaknesses with compliance provisions in 7% of the ISAs. In some cases, the ISA did not contain a requirement to notify ICBC of compliance issues. In others, the ISAs did not provide an authority for ICBC to audit compliance. Some ISAs lacked a stipulation that third parties provide annual compliance reports to ICBC. A few agreements permitted ICBC to request a review of policies and procedures but did not permit it to enter third party premises and inspect. Finally, there was one case where the ISA authorized ICBC to request external audits but only in the event of a breach.

RECOMMENDATION 2 (continued)

ICBC should include the following details in all ISAs:

h) The authority for ICBC to conduct compliance reviews, including inspections.

4.2.14 Termination & expiry

Nearly all (96%) of the sample of ISAs contain a clause for consequences should ICBC find that a third party is not compliant. In this event, ICBC may:

- suspend or request the suspension of an individual user's access to personal information;
- request additional safeguards be imposed by the third party on the individual;
- suspend the third party's access; or
- terminate the ISA.

Certain ISAs also note that ICBC may terminate the ISA at any time with or without cause.

All but five (95%) ISAs in the sample expire within three-to-five years, with three-quarters (77%) expiring at three years after signing. Third parties must request renewal of the ISA if they wish to continue access. The remaining 5% of sampled ISAs do not expire. These are:

- Medical Services Commission;
- Statistics Canada;
- Transportation Investment Corporation;
- CPIC; and

- CCMTA.

Each of these ISAs contain provisions for auditing ongoing compliance and two ISAs (the Medical Services Commission and CPIC) require a full review of the ISA every two to five years.

4.4 User access controls

ICBC provided the userIDs of individuals who have direct access to ICBC systems. These include ICBC employees, insurance brokers who act on behalf of ICBC, the BC Coordinated Law Enforcement Unit, and BC Government employees. BC government employees log in from their government workstations either directly to ICBC's mainframe with an ICBC-provided userID (referred to below as the "ministry list") or to the government mainframe that links to ICBC's mainframe with a userID provided by Shared Services (referred to below as the SSBC list).

Excluding ICBC employees and brokers, there were 2,125 unique userIDs in the inventory lists provided to OIPC auditors.

4.4.1 Currency and control of UserIDs

ICBC requires third parties with direct access to provide lists of authorized users when they initiate an ISA and annually thereafter. However, ICBC staff noted that third parties actually update user lists regularly when staff join or depart, and they provide updated user lists when ISAs are renewed.

Staff stated that ICBC creates userIDs after approving the ISAs. Third parties submit their user lists to ICBC and complete an access request form for their employees. ICBC then verifies the individual's authority to access information. Third parties use the same form to remove users.

PFOI staff told auditors that they review all requests for access or removal to ensure there is a valid ISA and then forward the request to ICBC's Information Access Management. ICBC staff stated that Information Access Management then verifies the access authority and forwards the request for approval to the Manager of PFOI. After the Manager of PFOI approves the request, ICBC sends a userID to the third party employee.

ICBC manages the ministry list and the government Shared Services (IT) team manages the SSBC list. ICBC relies on the Shared Services team to update the SSBC list and to allocate userIDs. ICBC staff reported that they thought the government also utilized a 90-day inactivity expiration policy.

OIPC auditors found, however, that the government does not utilize such a policy and does not keep the SSBC userID list up-to-date. ICBC provided the lists of userIDs for review. One-quarter (25%) of the active userIDs on the SSBC list had not been used for more than 90 days. Of these, 12% of the userIDs were last used in 2016 or early 2017 and the rest should have been revoked at some point between 2007 and 2015.

After further discussion, the Manager of Information Risk Management noted that they are not aware of any process to review or revoke inactive SSBC userIDs.

RECOMMENDATION 3

ICBC should require third parties to enforce a 90-day inactivity expiration policy and ICBC should monitor compliance.

OIPC auditors found no issues with the initial set-up procedures and ISA instructions for updating userIDs. However, auditors suggest that ICBC add a requirement in ISAs for third parties to immediately notify ICBC of suspended or terminated employees to enable ICBC to disable access for security purposes. ICBC could also require third parties to notify ICBC when employees take a long-term leave or move to a new work assignment, even if it is temporary.

RECOMMENDATION 4

ICBC should require third parties to update ICBC immediately upon the suspension, termination, or temporary departure of an employee.

4.4.2 Comparison of userIDs with ISAs

ICBC does not keep up-to-date userID lists that link individual employees to the ministry or the specific ISA. ICBC attempted to track userIDs by ISA or ministry but tracking became onerous due to frequent updates and changes to the user lists. There was also a limited capacity at ICBC to manage the lists.

For this reason, OIPC auditors were not able to confidently match the individual userIDs to a corresponding ISA. However, they were able to identify the ministry and branch for roughly half of the userIDs on the ministry list. The majority of the branches they could identify matched a corresponding ISA.

OIPC Auditors found two notable exceptions:

- The Receivables Management Office (RMO) in the Ministry of Finance and
- RoadSafetyBC in the Ministry of Public Safety and Solicitor General.

The Ministry of Finance currently has three ISAs with ICBC. One includes several branches that perform similar functions to the RMO (for example, collections, payments and taxation). ICBC could simply add the RMO to that ISA.

OIPC Auditors did not review the ISA with RoadSafetyBC because it is currently still a draft. Even without an approved ISA, FIPPA authorizes RoadSafetyBC to access personal information contained within all or any part of an individual's driving record.

ICBC noted that every userID should connect to an ISA, other than RoadSafetyBC. However, due to inconsistency in the user lists, OIPC auditors could not determine whether each userID with access to ICBC personal information was associated to an active ISA.

RECOMMENDATION 5

ICBC should catalogue the ISAs and keep track of userIDs by ISA.

RECOMMENDATION 6

ICBC should ensure an ISA is in place for every ministerial branch whose staff access the personal information collected by ICBC.

4.4.3 Duplicate UserIDs

The number of users for a ministry or branch depends on the role and function of individual users. OIPC auditors found the number of userIDs within each identifiable branch (and ISA) ranged from those with only one userID to ISAs with up to 109 userIDs.

There were 2,114 unique userIDs in the user lists. Of these, at least 345 individuals had two or more active userIDs. Three-quarters of these (76% or 262 individuals) had one userID on the ministry list and one on the SSBC list. This was not an issue because the ministry and SSBC lists provide two different avenues to access ICBC's personal information databases. Another 22 individuals had duplicate userIDs that contained a mistake. ICBC has since removed the mistaken userIDs.

However, OIPC auditors found at least 61 individuals with two or more active userIDs on the same list. At least 46 individuals had two or more userIDs through SSBC. Another 15 had two or more userIDs on the Ministry user list. One individual had four active userIDs on the SSBC list. These duplications suggest a deficiency in the security of direct access to ICBC databases by third parties.

The Manager of Information Risk Management noted that duplication in the ministry list could have resulted from ministries providing a name in an updated user list that does not exactly match the name ICBC previously used (e.g., partial first name or an initial instead full first name,

incorrect spelling, or nickname). In these cases, a user name search would not show a match. ICBC staff now conduct a detailed search for duplicate names when creating new userIDs.

The Manager of Information Risk Management was not able to confirm how duplicates occurred on the SSBC list, which the government's Shared Services manages. In some cases, Shared Services may have provided more than one SSBC userID to certain users in order to access different ICBC databases. The manager noted that this explanation does not apply to all of the SSBC duplicates.

Tools for monitoring user access, usage, and transaction volume are ineffective when individuals are able to access two or more accounts. ICBC systems are also susceptible to breaches, if users without a work purpose can continue to access them.

When OIPC auditors informed ICBC about the issues with the different userID lists, ICBC found and removed duplicates.

RECOMMENDATION 7

ICBC should regularly review its userIDs and remove duplicate and outdated userIDs.

4.5 Third party compliance monitoring and internal audit

Under FIPPA, public bodies are responsible for making reasonable security arrangements to protect the personal information in their custody or control against unauthorized access, collection, use, disclosure or disposal. Compliance monitoring and governance of ISAs is essential for ICBC to meet its obligations under s. 30 of FIPPA. As noted in ICBC's *Third Party Information Sharing Governance Plan/Program*, under FIPPA:

> Any time ICBC-held personal information is disclosed to or used by a third party, ICBC remains accountable for privacy compliance. As such, ICBC must have a robust Information Sharing Governance Program ("ISG Program") to ensure that it discloses personal information appropriately and in accordance with FIPPA and to help promote compliance by third parties with their statutory obligations and contractual obligations to ICBC.

In addition, the public expects that ICBC will protect the personal information it collects. A recent ICBC memo from Corporate Audit Services to PFOI linked the need for governance over ISA to stakeholder satisfaction:

> Governance over CPIC's access to ICBC data is required so that ICBC is informed of any breach or inappropriate use from access to customer information on a timely basis. Lack of governance may lead to negative media coverage for ICBC, as well as stakeholder dissatisfaction.[53]

OIPC Auditors recommend that governance should extend beyond CPIC agreements to the entire information sharing program.

In their 2013 compliance review, ICBC's Corporate Audit Services highlighted the lack of enforcement and monitoring of information sharing agreements. Since then, ICBC has started to address this issue.

In 2015, ICBC completed an initial risk assessment of third parties with indirect access and followed up with higher risk organizations. They also reviewed access provisions for third parties with direct access to ICBC systems. They compared the categories of personal information these users had the capability to access to the categories they actually used and reduced access accordingly.[54] As well, the IT system flags certain transactions that are out of the ordinary or high volume and they do ad hoc monitoring of VIP accounts.

OIPC auditors suggest that ICBC enhance system flags.

RECOMMENDATION 8

ICBC should enhance system flags and monitoring.

ICBC does not conduct compliance monitoring with those who have direct access to ICBC databases. Examples of appropriate compliance monitoring could include:

- auditing transaction records for each direct access third party on a rotating basis; and
- requesting those third parties to provide proof of the need for personal information.

In addition, ICBC does not track third party breaches or require the majority of third parties to report breaches involving ICBC-collected personal information. As previously noted, only 31% of ISAs reviewed required third parties to report breaches to ICBC.

Regarding ISAs and research agreements, one ICBC staff member said:

> People – for example researchers – are starting to realize that ICBC has one of the most complete data sets in BC and they want to use it for research or medical research purposes. That's a challenge with how you manage those requests and what our obligation is with regards to all this data. We are a Crown corporation and we perform many functions – like driver licensing – that in most provinces are performed by core

> government, so we have some obligation to provision data to other branches of government but it's really not clear what that obligation is, how far it goes, and how much of our resources to put into data sharing when it's not a core function of our business. It's becoming a bigger and bigger issue for us.

ICBC has planned to develop policies for direct access renewal since 2014. While they have accomplished certain aspects of the plan, competing priorities and limited resources have resulted in delays in others. To ensure compliance with FIPPA, ICBC needs to complete these activities and plan for regular compliance monitoring of ISAs. This will help ensure that third parties appropriately use and secure the personal information ICBC collects.

RECOMMENDATION 9

ICBC should conduct compliance reviews and inspections of third party access, collection, use, disclosure, or disposal of personal information.

RECOMMENDATION 10

ICBC should track and review breaches that occur at third party locations to ensure they are satisfied with prevention measures implemented prior to renewing an ISA.

RECOMMENDATION 11

ICBC should develop and/or consolidate policies on information sharing, managing requests and renewals, and governance of information sharing with third parties.

RECOMMENDATION 12

ICBC should conduct internal audits and reviews of the information sharing program (including regular review of policies, procedures and training).

5.0 RECOMMENDATIONS

The following recommendations result from the findings in this report. They comprise best practices that will help ICBC comply with legislative obligations to protect personal information.

To assist ICBC with implementation, the recommendations appear into the following thematic groupings:

- Information Sharing Agreements;
- User Access Provisions; and
- Compliance Monitoring.

RECOMMENDATIONS: INFORMATION SHARING AGREEMENTS

1. ICBC should prevent unauthorized disclosure of personal information to direct access third parties.
2. ICBC should include the following details in all ISAs:
    a. The legal authority for third party collection of personal information.
    b. The rationale for disclosure of each category of personal information, if it is not plain and obvious how the third party is entitled to collect or use the information.
    c. Identification of who has custody and control of personal information and at what point the custody or control changes.
    d. A requirement for third parties to have processes for managing and reporting breaches.
    e. A requirement for third parties to have written procedures to resolve complaints about their information-handling practices.
    f. A requirement for third parties to have a written privacy policy.
    g. A requirement for third parties to provide privacy and security training to staff prior to gaining access to personal information collected by ICBC.
    h. The authority for ICBC to conduct compliance reviews, including inspections.

RECOMMENDATIONS: USER ACCESS PROVISIONS

3. ICBC should require third parties to enforce a 90-day inactivity expiration policy and ICBC should monitor compliance.
4. ICBC should require third parties to update ICBC immediately upon the suspension, termination, or temporary departure of an employee.
5. ICBC should catalogue the ISAs and keep track of userIDs by ISA.
6. ICBC should ensure an ISA is in place for every ministerial branch whose staff access the personal information collected by ICBC.
7. ICBC should regularly review its userIDs and remove duplicate and outdated userIDs.

RECOMMENDATIONS: COMPLIANCE MONITORING

8. ICBC should enhance system flags and monitoring.
9. ICBC should conduct compliance reviews and inspections of third party access, collection, use, disclosure, or disposal of personal information.
10. ICBC should track and review breaches that occur at third party locations to ensure they are satisfied with prevention measures implemented prior to renewing an ISA.
11. ICBC should develop and/or consolidate policies on information sharing, managing requests and renewals, and governance of information sharing with third parties.
12. ICBC should conduct internal audits and reviews of the information sharing program (including regular review of policies, procedures and training).

6.0 CONCLUSION

The ability for individuals to control their own personal information is fundamental to protecting privacy under FIPPA and is a right that citizens value. Therefore, public bodies need to have appropriate controls in place to protect the personal information they hold. They must also limit disclosure of that personal information to circumstances authorized by FIPPA.

ISAs detail the public body's expectations for protecting personal information when shared with third parties and help public bodies meet their obligations under s. 30 of FIPPA.

Based on the sample of ISAs, auditors found that ICBC has the appropriate authority under FIPPA to disclose personal information for the purposes identified in each of the ISAs. The disclosure of personal information is generally reasonable and proportionate for the intended use by third parties. Auditors also found that the majority of ISAs contain the essential components.

ICBC could do more to protect personal information by:

- amending ISAs, when they are up for renewal, to incorporate collection authority, rationale for disclosure, custody and control, breach management, training and notification to ICBC in the event of staff termination;
- tracking and reviewing third party access to personal information held by ICBC, including removing duplicate and outdated userIDs, and ensuring that an ISA is in place before granting access to third parties; and
- conducting additional compliance monitoring with third parties as well as internal audits and reviews of ICBC systems, policies, and information sharing governance.

Compliance monitoring and effective governance of information sharing is critical for the protection of personal information. In order to meet their obligations under FIPPA, ICBC should increase compliance monitoring of their own practices, as well as with those of the third parties with whom they share information.

ICBC's executive should ensure that appropriate resources are available to develop, implement, and adapt the program.[55] Executive commitment, which is at the heart of a privacy-respectful culture, is required to ensure ICBC actively incorporates these essential components into its privacy management program.

7.0 ACKNOWLEGEMENTS

I would like to thank Tanya Allen, Audit Manager, and Gbola Atitebi, Audit Researcher, who conducted the audit and drafted this report.

September 13, 2017

Drew McArthur
Acting Information and Privacy Commissioner
for British Columbia

APPENDIX A: METHODOLOGY

This audit focused on ICBC's compliance with FIPPA provisions relating to the collection, use, disclosure, protection, and retention of personal information by public bodies in accordance with Part 3 of FIPPA.

This project utilizes compliance assessment, operational audit, program evaluation, and process improvement methodologies and included the following components:

1. Review of ICBC policies and practices on sharing and protecting personal information of drivers, vehicle owners, and insurance policy holders;
2. Examination of a sample of ICBC ISAs;
3. Analysis of ICBC user lists to determine the third parties that have access to databases containing personal information;
4. Verification of ISAs where third parties have database access; and
5. Interviews with select ICBC staff.

OIPC auditors built assessment criteria and tools based on FIPPA obligations, OIPC guidance documents and orders, and ICBC's information sharing policies and procedures.

This audit has four objectives:

1. Review the extent to which ICBC processes and ISAs reflect legislative requirements;
2. Examine third party access to the personal information of drivers, vehicle owners, and insurance policy holders;
3. Identify any risk factors in the protection of personal information; and
4. Formulate recommendations to strengthen ICBC policy and practice.

Lines of inquiry for this audit are whether ICBC:

- has an adequate policy framework relating to the approval, drafting, and monitoring of ISAs;
- has met its obligations under FIPPA, OIPC guidance documents and orders, and ICBC policies relating to the collection, use, disclosure, protection, and retention of personal information; and
- protects personal information as required by s. 30 of FIPPA.

7.1 Background research

OIPC auditors reviewed the following documents for use in the creation of assessment criteria and tools and to gain an understanding of the background and context of ICBC's information sharing activities and agreements.

- Statistics Canada *Audit of Data Sharing Agreements: Ontario Ministry of Health and Long Term Care*, published March 2012.
- Statistics Canada *Audit of Data Sharing Agreements: BC Ministry of Health*, published April 22, 2013.
- Treasury Board Secretariat *Guidance on Preparing Information Sharing Agreements Involving Personal Information*, published July 2010.
- Saskatchewan IPC *Best Practices for Information Sharing Agreements*, published September 2014.
- Alberta OIPC *Guide for Developing Personal Information Sharing Agreements*, published October 2003.
- OIPC *BC Physician Privacy Toolkit* section on "Managing Contracts and Information Sharing Agreements," published June 2009.
- OIPC *Guidelines for Data Services Contracts*, published May 2003.
- OIPC *Guidelines for Audits of Automated Personal Information Systems*, published October 2001.
- OIPC orders and other case files involving ICBC:
    - OIPC Mediation Summary P16-01-MS *Sharing Information for Debt Collection Purposes*, published January 2016.
    - OIPC Investigation Report F12-01 *Investigation into the Use of Facial Recognition Technology by ICBC*, published February 2012.
    - OIPC Investigation Report P95-005 *Cars, People and Privacy: Access to Personal Information through the Motor Vehicle Data Base*, published March 1995.
    - An additional 24 files received by the OIPC between 2012 and 2016, including complaints (11 files), policy issues or consultations (5 files), privacy impact assessments (3), breach notifications (3), and project or internal reviews of issues related to information sharing activities (2).
- Past audits or reviews of ICBC third party disclosures or ISAs:
    - Deloitte *Assessment of controls related to customer personal information access for Claims Adjusters*, published November 2011.
    - ICBC's Privacy Compliance Review, published December 2013.

- ICBC Corporate Audit Services *Governance over Providing Personal Information to Third Party Agencies*, numerous reports published September 2014 to December 2016.

7.2 Review of policies and procedures

This portion of the review included an overview of the ICBC policies, procedures, and other documentation to understand and report on the process for evaluating, approving, and establishing ISAs.

OIPC auditors reviewed the following materials:

- ICBC policies and other documentation relating to IT security, PIAs, breach management, records retention, and personal information disclosures;
- Access request approvals and renewals and ISA templates;
- Internal audit and compliance activities;
- Lists of ISAs with direct and indirect access and CPIC-related; and
- Lists of systems and databases where personal information is stored and may be accessed or disclosed to third parties through direct or indirect means.

OIPC auditors also used materials they collected during this portion of the review to create interview guides and checklists for reviewing ISAs.

7.3 Interviews

In addition to the examination of requested documents ICBC provided, OIPC auditors conducted a preliminary interview in March 2017 with ICBC's Manager of PFOI, in-house privacy Legal Counsel (Corporate Law), and Manager of Information Risk Management. The two-hour interview included questions on:

1. application and approval processes for information sharing;
2. decisions on ISAs vs. other agreements, contents of ISAs, and recent changes;
3. security safeguards; and
4. compliance monitoring.

OIPC auditors conducted a follow-up interview in June 2017 with the Manager of PFOI, the Manager of Information Risk Management, and individuals from ICBC's Corporate Audit Services.

OIPC auditors used information from the preliminary interview to develop a basic understanding of ICBC processes with regard to information sharing. OIPC auditors used

information collected during the follow-up interview to clarify findings from the review of policies and procedures and the audit ISAs.

7.4 File audits

The audit of ISAs included:

- a census of ICBC's direct access ISAs (n=27); and
- a random sample of indirect access ISAs, CPIC ISAs, and ISAs with other government agencies (n=71).

7.4.1 Random sample of indirect ISAs

Using standard statistical methods, OIPC auditors selected the random sample of 71 ISAs. This size of sample provides a four percentage point margin of error (MOE) at a 95% confidence level, meaning that the sample selected for review will provide an accurate representation of the overall population of ICBC ISAs, within four percent, 19 times out of 20. In some cases, the MOE ranged from a low of two percent to a high of eight percent, depending on the aspect of analysis.

OIPC auditors conducted a comparison of key demographics between the sample and the population of files to ensure that the sample reasonably mirrored the overall population of ISAs on variables such as length of agreement term and type of agency.

OIPC auditors selected a smaller sample during this audit because ICBC drafts its ISAs from a template, creating a similar format across the agreements. As such, OIPC auditors hypothesized that findings of gaps or areas for improvement with ISAs would be relatively similar or common across the population of ISAs. Results confirmed this hypothesis.

7.4.2 Analysis of direct and indirect ISAs

In total, OIPC auditors reviewed 98 ISAs and analyzed findings from 94. During review, auditors removed the following four ISAs of public bodies and organizations from the analysis:

- The ISA with RoadSafetyBC, which was still in draft form upon completion of the data collection;
- One ISA with a vehicle repair shop that ICBC was unable to locate (the ISA was re-drafted during the course of the review);
- The agreement with the Tuberculosis and Chest Disabled Veterans Association (TBVets), which government grandfathered into FIPPA at the onset of the legislation, did not comprise a formal ISA; and
- An agreement with the BC Ministry of Employment & Income Assistance, which was for emergency access services rather than information sharing.

OIPC auditors reviewed the ISAs in relation to 73 different points of data. Examples of these data points include:

- type of personal information;
- the stated purpose for disclosing each type of personal information;
- legal authority to permit ICBC disclosure and third party collection;
- whether notification for the disclosure was to be provided or consent obtained;
- the mode, frequency, and duration of sharing;
- who and how access is provided (e.g., how does ICBC determine the individual requesting access is the appropriate representative of the third party);
- required physical and electronic security measures;
- third party retention periods and destruction of personal information;
- breach and incident management;
- limits to collection, use and disclosure;
- accuracy and correction of personal information;
- indemnification clauses;
- compliance monitoring provisions;
- training requirements;
- term and expiry of agreement;
- restrictions on foreign disclosure or storage of personal information;
- consequences to non-compliance with agreements;
- renewal processes; and
- identification of data custodian and the custody and control of the personal information disclosed by ICBC and collected by third parties.

OIPC auditors then evaluated and cross-tabulated these data points to establish findings for inclusion in the report and create interview guides for follow-up interviews with ICBC staff.

7.5 Comparison of direct access users with ISA lists

ICBC provided user lists of all individuals with direct access to ICBC systems that contain personal information. Two main lists comprised the majority of userIDs: the Ministry list (managed by ICBC) and the SSBC list (managed by the government). OIPC auditors combined the two lists and separated out user names (first name and last name), ministry names or abbreviations, and branch names or abbreviations, where possible.

In the ministry list, OIPC auditors were only able to identify and confirm the branches for half (50%) of the userIDs. Auditors then compared those branches to the list of ISAs and were able to match 59% of the identifiable branches with a specific ISA. This means that OIPC auditors could only match an existing ISA to 39% of the userIDs on the ministry list. It is probable that more than 39% of the userIDs on the ministry list are associated with an ISA but, based on available information, further matching is not possible.

OIPC auditors then reviewed the combined list to look for duplication. They marked userIDs by duplicate last name and then, where a duplicate last name occurred, by duplicate first name. They then reviewed the data manually to mark likely duplications where first names appeared incomplete in the data. For example, OIPC auditors would have considered “Ste Parker” to be a duplicate of “Steven Parker.” As noted in the report, a number of duplications existed in the ICBC user lists.

OIPC auditors then removed duplicate users who had only one userID on the ministry list and one on the SSBC list and looked for duplications within the same list. As noted, duplication continued to exist on the same lists. OIPC auditors then analyzed the SSBC list based on the last occasion of access by that userID and found that ICBC should have applied the expiration policy and revoked a number of active userIDs.

OIPC auditors used this information to establish findings for inclusion in this report and to create the follow-up interview guide with ICBC staff.

ENDNOTES

[1] ICBC. *Company Information.* http://www.icbc.com/about-icbc/Pages/default.aspx.

[2] For example, s. 19 of the *E-Health Act* and s. 67 of the *Coroners Act*, prescribe the content for ISAs entered into under those statutes.

[3] College of Physicians and Surgeons of British Columbia, Doctors of BC, and OIPC. 2017. *BC Physician's Toolkit*. https://www.oipc.bc.ca/guidance-documents/1470. Please note, this link currently leads to the 2009 version of the document but will soon be updated.

[4] ICBC. 2016. *Protecting the Privacy of Personal Information Policy*. P 5.

[5] ICBC. *MV2645 Interim Driver Licence Form.*

[6] ICBC. APV, Owner's Certificate of Insurance and Vehicle Licence APV250 Form.

[7] Formerly the Office of the Superintendent of Motor Vehicles. RoadSafetyBC is responsible for road safety and strategic direction throughout British Columbia. http://www2.gov.bc.ca/gov/content/transportation/driving-and-cycling/road-safety-rules-and-consequences/organizational-structure-and-partnerships/our-partners#overview.

[8] ICBC. *Privacy Policy – About ICBC.* http://www.icbc.com/about-icbc/Pages/Our-privacy-policy.aspx.

[9] ICBC. *Access to Information Review Committee – Guidelines for review of new and existing Direct Access Agreements.* P 1.

[10] ICBC. 2011. *Access to Information Review Committee Terms of Reference*. P 1.

[11] ICBC. 2011. *Access to Information Review Committee Terms of Reference*. P 1.

[12] ICBC. 2011. Access to Information Review Committee Terms of Reference. P 2.

[13] ICBC. 2017. Email communication from Manager, Privacy and FOI. April 11, 2017.

[14] ICBC. *Access to Information Review Committee – Guidelines for review of new and existing Direct Access Agreements*, undated. The AIR Committee guidelines are not an official policy or procedure; however, the Manager, Privacy and FOI reported via email during the audit that the AIR Committee still follows the general principles found in the document.

[15] ICBC. 2015. *Access to Information Review Committee Minutes.* March 19, 2015.

[16] ICBC. *Access to Information Review Committee – Guidelines for review of new and existing Direct Access Agreements*. P 1.

[17] It appears that police may have access both through direct and indirect methods. Police have access to ICBC information directly through their link to the Canadian Police Information Centre (CPIC) and through ICBC's Police Line program with handles roughly 30,000 calls per year. See ICBC. *DTVI Indirect Access Information Sharing Procedures*. P 2.

[18] ICBC. 2015. *Third Party Compliance Review (TCR) Program*. P 1.

[19] ICBC. *DTVI Indirect Access Information Sharing Procedures*. P 2.

[20] ICBC. *DTVI Indirect Access Information Sharing Procedures.* P 4.

[21] ICBC. 2016. *Verification Procedure*.

[22] ICBC. 2015. *Third Party Compliance Review (TCR) Program.* P 1.

[23] ICBC Corporate Audit Services. 2014. *Governance over Providing Personal Information to Third Party Agencies. P* 4.

[24] ICBC Corporate Audit Services. 2014. *Governance over Providing Personal Information to Third Party Agencies. P* 4.

[25] ICBC. 2014. *Access to Information Review Committee Minutes*. December 16, 2014.

[26] ICBC. 2016. *Protecting the Privacy of Personal Information Policy*, Principle 8 "Security of Personal Information." P 8.

[27] ICBC. 2016. *Protecting the Privacy of Personal Information Policy*. P 1.

[28] ICBC. 2013. *Information Governance at ICBC*. P 3.
[29] ICBC. 2013. *Technical Vulnerability Management Standard*. P 2.
[30] ICBC. 2013. *Privacy Breach Guidelines* December 2013.
[31] ICBC. 2014. *Information Systems Security.* P 6.
[32] ICBC. *Security Incident Reporting Standard* Part 2 "Standard." P 2.
[33] ICBC. *Security Incident Reporting Standard* Part 2 "Accountabilities." P 2.
[34] ICBC Corporate Audit Services. 2014. *Governance over Providing Personal Information to Third Party Agencies*. P 5.
[35] ICBC. 2013. *Privileged Access Security Standard*.
[36] ICBC. 2014. *Information Systems Security.*
[37] ICBC. 2014. *Information Systems Security.* P 11.
[38] ICBC. 2014. *Information Systems Security.* P 9.
[39] ICBC. 2014. *Information Systems Security.* P 8.
[40] ICBC. 2014. *Information Systems Security.* P 2.
[41] ICBC. 2016. *Password Creation and Management Standard*. P 2.
[42] ICBC. 2015. *Third Party Compliance Review (TCR) Program.* P 3.
[43] ICBC. 2014. Information Security Requirements Standard. P 2.
[44] ICBC. 2013. *Privacy Compliance Review* (2013).
[45] ICBC. 2013. *Privacy Compliance Review* (2013). P 7.
[46] ICBC Corporate Audit Services. 2014. *Governance over Providing Personal Information to Third Party Agencies: Executive Summary Report*. Pp. 2-3.
[47] ICBC Corporate Audit Services. 2014. *Governance over Providing Personal Information to Third Party Agencies*. *Executive Summary Report*. P 5.
[48] ICBC. 2015. *Third Party Compliance Review Program.*
[49] ICBC. 2015. *Third Party Compliance Review (TCR) Program*. P 5.
[50] College of Physicians and Surgeons of British Columbia, Doctors of BC, and OIPC. 2009. *BC Physician's Toolkit*. https://www.oipc.bc.ca/guidance-documents/1470.
[51] Several ISAs had multiple uses listed, so results add up to more than 100%.
[52] ICBC. 2014. *Information Systems Security.* P 9.
[53] ICBC. 2016. *Governance of CPIC Access to ICBC-Managed Information*.
[54] ICBC. 2017. Email communication from Manager, Information Risk Management. June 27, 2017.
[55] OIPC. 2013. "Accountable Privacy Management in BC's Public Sector." https://www.oipc.bc.ca/guidance-documents/1545.