

MINISTRY OF CITIZENS' SERVICES AND OPEN GOVERNMENT MINISTER'S TRANSITION BINDER

Table of Contents

TAB

Ministry Overview	1
Overview	A
Executive Team	B
Divisional Summaries	C
Org Chart	D
Key Roles and Responsibilities	2
Asset Sales	A
BC Online	B
Citizen Centred Service Delivery	C
Device Strategy	D
Digital Services Strategy	E
FOI Administration	F
Government Reorganization	G
Identity Management/BC Services Card	H
Leading Workplace Solutions	I
Network BC	J
Open Government	K

Security and Privacy	L
Shared Services BC	M
Strategic Partnerships Office	N
Legislation and Policy	3
Freedom and Information and Protection of Privacy Act	A
Naming Opportunities	B
Other Legislation	C
Budget	4
Overview	A
2013/14 Budget	B
Capital Program	C
Shared Services Funding Model	D
Major Contracts	E
Strategic Telecommunications Services Deal	F
30, 60, 90 Day Decisions	5
Platform Commitments	6
Office of the Chief Information and Privacy Commissioner	7
Crowns, Boards and Agencies	8
Stakeholders	9
Service Plan	10

DIVISIONAL SUMMARY

Logistics and Business Services

Overview and Major Accountabilities

The Logistics and Business Services division (LBS) has 555 staff in eight cities across the province (Victoria, Coquitlam, Kamloops, Kelowna, Nanaimo, Nelson, Prince George, and Surrey). There are three major business areas: Information Access Operations, Procurement Services, and Supply Services.

Information Access Operations

Information Access Operations (IAO) is a highly transactional, citizen-facing operation. The role of the Freedom of Information department is to respond on behalf of ministries to 10,000 requests from citizens, approximately half of which are for personal information, and half of which are for general information. IAO is also responsible for posting responses to government's general FOI requests, and travel expense summaries of senior government officials. Around half of all general requests are posted online on government's Open Information website.

The Government Records Service team plays a key role in the management of government's records processes. There are 950,000 boxes of government records currently in storage and approximately 55,000 new boxes are sent to storage each year.

Not Responsive

Pages 4 through 6 redacted for the following reasons:

S13

DIVISIONAL SUMMARY

Office of the Chief Information Officer

Overview of Major Accountabilities

The Office of the Chief Information Officer (OCIO) plays a leadership role in promoting and guiding the management of government information as a strategic business asset, and supporting technology infrastructure as a key enabler of business transformation.

The OCIO is responsible for the following core functions:

Not Responsive

Not Responsive

Legislation, Privacy and Policy Branch

The Legislation, Privacy and Policy Branch (LPP) is responsible for managing changes to, and providing advice on, IM/IT legislation and policy including: the *Freedom of Information and Protection of Privacy Act*; the *Personal Information Protection Act*; the *Electronic Transaction Act*; the *Document Disposal Act*; Chapter 12 (Information and Technology Management) of the Core Policy and Procedures Manual; and the Naming Privileges Policy. LPP develops supporting policies, standards, guidelines, operational tools business processes and training material to assist public bodies and private sector agencies in understanding their obligations under these Acts and policies.

LPP is responsible for reviewing Privacy Impact Assessments, Information Sharing Agreements, Research Agreements and Privacy Protection Schedules in government contracts to ensure compliance with privacy legislation and policy and for investigating privacy breaches that occur within government, providing immediate support, containment and remediation strategies.

Not Responsive

Page 9 redacted for the following reason:

S13

Not Responsive

S13

Not Responsive

OPEN GOVERNMENT

Lead Executive

Jay Schlosar, Assistant Deputy Minister, Strategic Initiatives Division

Background

On July 19, 2011, the Province launched the Open Government agenda as a means to demonstrate greater government transparency, encourage engagement in public decisions, and drive innovation in public services. The Open Government agenda encompasses four distinct but related initiatives:

Not Responsive

- **Open Information**, which enhances openness and transparency through the public release of information about government;

Not Responsive

While these initiatives are primarily understood under the brand of “Open Government,” they also represent a number of the core programs behind the strategic shifts outlined in *Citizens @ the Centre* – in particular, Citizen Participation and Self-Service (see Key Roles and Responsibilities: Transformation and Technology Planning for more information).

British Columbia has been acknowledged through multiple awards for its open government efforts, including: the Institute of Public Administration in Canada’s (IPAC) 2011 Public Sector Leadership Award, the 2012 ESRI Special Achievement award in geographic information systems (GIS), and a 2012 GTEC Distinction Award. In April 2012, the independent Stratford institute announced that British Columbia was ranked first in Canada for e-government as a result its efforts on open government.

Current Context

Not Responsive

¹ All programs are overseen by the Strategic Initiative Division, with the exception of the Open Information program, which is overseen at a policy-level by the Strategic Initiatives Division but is operated through the Information Access Operations branch under the Logistics and Business Services Division due to the alignment with existing FOIPPA processes.

Not Responsive

Open Information

The Open Information program (www.openinfo.gov.bc.ca) provides citizens with access to information about government. In particular, this program encourages ministries to routinely

release information about decisions and operations, and to encourage the greater sharing of information that is currently only available through the Freedom of Information (FOIPPA) process. Alongside supporting a corporate culture shift, the program specifically delivers new types of information to the public that were previously not made widely available, in two ways:

1. Routinely releasing monthly reports on travel expense accrued by Ministers and Deputy Ministers in the course of their duties.
2. Supporting the proactive disclosure of complete general information requests requested by applicants through the Freedom of Information office, and provides them to the public 72 hours after they are released to applicants (subject to policy).

Since the Open Information Program was created in July 2011, it has:

- Launched the Open Information site, which allows citizens to access both routinely released cross-government information (Ministers and Deputy Ministers' travel expenses) and responses to general Freedom of Information requests
- Developed policy that establishes a corporate governance framework for the proactive and routine release of information, and made amendments to the *Freedom of Information and Protection of Privacy Act* to support those activities.
- Released over 3,000 items (approximately 2,000 FOI response packages and 1000 expense summaries), resulting in over 55,000 site visits and 51,000 downloads (as of March 31/13)

Not Responsive

Not Responsive

S13

SECURITY AND PRIVACY

Office of the Chief Information Officer

Lead Executive

Bette-Jo Hughes

Background

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) establishes the legislative privacy framework for government. It formalizes a set of rules for collecting, using and disclosing personal information. It also establishes an independent Information and Privacy Commissioner (Commissioner) with the power to investigate privacy complaints made against government, to initiate reviews or audits and make public comment respecting the privacy implications of any proposed initiative, program or activity of government.

FOIPPA also establishes security obligations for government by requiring that reasonable security arrangements be in place to protect personal information in its custody or under its control. Reasonableness is a sliding scale, assessed relative to the sensitivity of the personal information in question and other factors. Government Information Security Policy, which is based on the international standard ISO27002-2005, specifies what “reasonable” security means for both personal and other confidential information and sets policies respecting the appropriate tools, systems and controls for managing and transmitting this sensitive information.

Key Responsibilities

The Office of the Chief Information Officer (OCIO), represented by the Legislation, Privacy and Policy Branch (LPP) and the Information Security Branch (ISB), is responsible for developing legislative and regulatory changes to FOIPPA; establishing government’s privacy and security policies and standards; monitoring compliance with those policies and standards; managing government’s privacy training program; and investigating privacy and security breaches. Ministries are responsible for protecting the personal and other confidential information they hold or are responsible for (including information held by service providers) in accordance with FOIPPA and government policies and standards. Ministries are also accountable for any breach or failure to comply with legislation, policy or standards.

To assist ministries in meeting their privacy and security obligations, LPP and ISB conduct outreach activities and provide training, resources, guidance and support to ministry programs and projects. For example, when ministries are developing new legislation, programs, projects or systems, they are legislatively required to complete a Privacy Impact Assessment and submit

it to LPP for review. They must also conduct a Security Threat and Risk Assessment on projects, programs and systems in consultation with ISB. LPP also assists ministries with Information Sharing Agreements, Research Agreements and contract-based Privacy Protection Schedules.

Current Context

While LPP and ISB are distinct branches with distinct mandates, they collaborate in a number of areas and provide coordinated advice and support to corporate programs and ministries to assist them in meeting their privacy and security obligations.

Joint Activities

LPP and ISB are currently providing ongoing support and guidance to corporate initiatives such as identity information management projects, the BC Services Card Program, the Device (and BYOD) Strategy and Integrated Case Management. In recent consultations with the Office of the Information and Privacy Commissioner (OIPC) on the privacy framework for the BC Services Card, the Commissioner requested comprehensive documentation of the project's security features for review by a security expert. It is anticipated that this will be the standard expected for future projects and will require more extensive collaboration between LPP and ISB to provide the Commissioner with the information she deems necessary to determine whether a project is compliant with FOIPPA.

LPP and ISB also work together to conduct investigations into reported information incidents, which include actual or suspected privacy and security breaches. ISB also investigates cyber-attacks against government information technology infrastructure and supports the BC Public Service Agency in conducting investigations into actual or suspected instances of misconduct by public service employees. During 2012, ISB conducted more than 500 information security investigations and LPP conducted 777 investigations of confirmed privacy incidents.

LPP and ISB co-host an annual Privacy and Security Conference, which this year attracted over 850 delegates from across North America and featured over 60 presentations by national and international experts. This internationally recognized conference positions British Columbia as a leader in privacy and security matters of global importance.

Ministry Contacts

One area of difference between the privacy and security areas is the level of organizational maturity. For instance, at present each ministry has a dedicated Ministry Information Security Officer which is a point of contact and has responsibility for ensuring and supporting security compliance within the ministry. Until several years ago, each ministry also had a dedicated privacy officer. However, this responsibility was centralized to LPP, with the result that there is no longer a dedicated resource within each ministry to support and ensure privacy compliance. Currently, LPP liaises with the Ministry Chief Information Officers and is in the process of

developing a Privacy Community of Practice which would include representatives from each ministry and would provide a forum for addressing emerging privacy trends and issues, disseminating information on new policies, problem solving specific ministry issues and sharing successful approaches and solutions.

Compliance and Monitoring

Security has a more mature compliance and monitoring program relative to privacy. ISB operates a Corporate Information Risk Reporting Program, which captures information about corporate information security risks, and also has the ability to conduct proactive security audits of ministries or specific program areas. In comparison, LPP is in the early stages of formalizing a comprehensive privacy management program that would incorporate compliance and monitoring components.

Major Activities in 2013/14

Over the coming year, LPP and ISB will continue to expand their outreach activities and enhance their operational tools, guidelines and training to better empower ministries to protect privacy and security. Both branches will also continue to provide advice and policy support to the Device (and BYOD) Strategy and Phase 2 of the BC Services Card Project. In addition, the following major activities will be a priority for 2013/14:

S13

Not Responsive

-
3. **New Privacy Impact Assessment directions, guidelines and templates:** LPP is currently developing new Privacy Impact Assessment directions, guidelines and templates in consultation with the Commissioner's office. The new directions, templates and guidelines will streamline the privacy assessment process for ministries, while at the same time providing for a more comprehensive assessment that will enhance government's compliance with FOIPPA and facilitate public bodies' consultations with the Commissioner. These new templates and processes will be completed and implemented by Fall 2013.
 4. **Privacy and Security Conference and other events:** LPP and ISB will host the 15th Annual Privacy and Security Conference in February 2014. ISB will also host the National Chief Information Officers' Committee on Information Protection in May 2013.

THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Legislative, Privacy and Policy, Office of the Chief Information Officer

Background

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) came into force in May of 1992 and was proclaimed in stages from 1993 to 1994, extending the Act to an expanded set of public bodies with each stage. FOIPPA currently covers over 2,900 public bodies, which fall into four general categories: (1) ministries; (2) crown corporations, agencies, boards and commissions; (3) local public bodies (such as municipalities, health authorities, school boards and universities and colleges); and (4) governing bodies of professions or occupations (such as the College of Physicians and Surgeons).

The purpose of FOIPPA is two-fold: (1) to make public bodies more accountable to the public by providing the public with a right of access to information, subject to limited exceptions; and (2) to protect personal privacy by prohibiting the unauthorized collection, use or disclosure of personal information by public bodies.

The Information and Privacy Commissioner (Commissioner), an independent Officer of the Legislature, has responsibility for overseeing and monitoring how FOIPPA is administered and for ensuring that its purposes are achieved. In addition, a legislatively-mandated Special Committee to Review FOIPPA is struck every six years to review and make recommendations for changes to the Act.

FOIPPA has been the subject of review by three Special Committees of the Legislative Assembly. It has been amended a number of times since 1992, most recently in the fall of 2011.

The 2011 Amendments to FOIPPA

The November 2011 amendments were the most significant set of amendments made to FOIPPA since its introduction in 1992. These amendments modernized the Act by enabling the delivery of more integrated, online and citizen-centric services and by authorizing new ways of communicating with citizens through the use of emerging technology such as social media. They also established a legislative framework for government's open information and open data initiatives and its identity information management initiatives, and implemented a number of recommendations made by the Special Committees. Other amendments strengthened

requirements for Privacy Impact Assessments, introduced new requirement for data linking and increased the Commissioner's oversight powers.

Several amendments were dependent on the implementation of regulations, directions and other instruments for full effect. The amendments also required that many of these supporting instruments be developed in consultation with the Commissioner. S12

S12

Amendments to the FOIPP Regulation

Amendments to the FOIPP Regulation were passed in June 2012 and included regulations that: (1) supported the 2011 amendments to FOIPPA (e.g., authority for collection of personal information with consent; documentation necessary to establish a common or integrated program) and (2) implemented the Special Committee recommendations on fees and who may act for others under FOIPPA. The Commissioner was consulted on all of these amendments.

S12

S13

S13
S12

Open Information and Open Data

The 2011 amendments authorized the Minister responsible for the Act to establish categories of records that ministries must disclose without a request under FOIPPA and to issue directions to ministries regarding disclosure of these categories of records. To date, no directions have been issued, beyond the Premier's direction on Open Information and Open Data which was

issued in July 2011. The Ministry's Strategic Initiatives Division is leading the development of guidance for ministries on categories of records that should be disclosed on a routine basis and is consulting with the Commissioner on this initiative. At this point, no decision has been made on whether additional directions will be necessary to support government's Open Information and Open Data initiatives.

Information Sharing Code of Practice

The 2011 amendments introduced a new requirement for the Minister responsible for the Act to establish, in consultation with the Commissioner, an Information Sharing Code of Practice. The Code of Practice will make recommendations to public bodies on the appropriate exchange of personal information and will not require drafting by Legislative Counsel or approval by Cabinet. Development of the Code of Practice is underway, with a plan to complete it in late 2013 or early 2014.

Future Amendments

S12

A. Enactments for which CITZ has legislative responsibility and is the Program Owner

Act Name	Description	Owner
	Not Responsive	
Freedom of Information and Protection of Privacy Act	Sets out the public's right of access to Information from public bodies, subject to limited exceptions, and protects personal privacy by prohibiting the unauthorized collection, use or disclosure of personal information by public bodies.	Legislation, Privacy and Policy, OCIO
	Not Responsive	

LEGISLATION

Background

The Ministry of Citizens' Services and Open Government (CITZ) is responsible for 32 pieces of legislation, which can be categorized as follows:

- A. Acts related to Information Management/Information Technology (IM/IT) including the *Freedom of Information and Protection of Privacy Act (FOIPPA)*, the *Personal Information Protection Act (PIPA)*, the *Document Disposal Act (DDA)*, and the *Electronic Transactions Act (ETA)*;

Not Responsive

S12

Not Responsive

S12

Not Responsive

30, 60, 90 Day Decisions

Issue: Issues related to FOIPPA and the Office of the Information and Privacy Commissioner

- There are some outstanding policy issues for government related to the Freedom of Information and Protection of Privacy Act (FOIPPA) and related topics outstanding with the Information and Privacy Commissioner (OIPC).

Background

- Investigation into no records responses:
 - As part of her investigation into government's no record response, the OIPC made six recommendations to government. Five of those recommendations are underway within the Ministry of Citizens' Services and Open Government.
 - A sixth recommends that government create a legislated duty within FOIPPA to document key actions and decisions. Government's response in March 2013 was that this would be referred to the next Special Committee on FOIPPA.
- Open government report:
 - In 2011 the OIPC announced that they would no longer report annually on government's timeliness in response to FOIs since the achievement levels were high.
 - Instead, the OIPC would report annually on open government.
 - The first open government report has yet to be produced by OIPC but is currently expected in the summer of 2013.
 - While government has achieved success on its open data program and national recognition on its leadership in open government, the Commissioner is expected to recommend new areas of pursuit in open information, specifically in the proactive release of government information.

Not Responsive

- Data Linking:
 - Amendments were introduced to FOIPPA in the fall of 2011.
 - The amendments were the result of extensive consultation with OIPC.

- As part of the amendments, the Commissioner has oversight into data linking initiatives.

S13

Decision Required

- It is expected that the Information and Privacy Commissioner will raise these policy topics and may issue the reports noted during the first 60 days of government's mandate.

THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

OFFICE OF THE CHIEF INFORMATION OFFICER

Background

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight and enforcement of British Columbia's access to information and privacy laws, which include:

- The *Freedom of Information and Protection of Privacy Act* (FOIPPA) which covers government ministries and over 2,900 other public bodies; and
- The *Personal Information Protection Act* (PIPA) which covers over 300,000 B.C. businesses, associations, trade unions, charities and trusts.

The Information and Privacy Commissioner (Commissioner) is appointed as an independent Officer of the Legislature with a renewable six-year term.

Mandate

FOIPPA and PIPA provide a broad mandate for the Commissioner. This mandate includes investigating and resolving access to information and privacy complaints; initiating investigations and audits of public bodies' and private organizations' compliance with FOIPPA and PIPA, educating the public about their access and privacy rights; and commenting publicly on the access or privacy implications of a public body or private sector program or initiative.

The Commissioner routinely provides commentary on the access and privacy implications of large scale programs, such as the BC Services Card; new legislation; sensitive or large-scale privacy breaches; and any proposed amendments to FOIPPA or its Regulations.

Recent changes to FOIPPA have further expanded this mandate, providing the Commissioner with more visibility into, and earlier notification of, public bodies' planned data-linking and information sharing initiatives. Public bodies must now provide the Commissioner with early notice of their intent to establish a common or integrated program or a data linking initiative with another public body or agency. They must also follow up with a privacy impact assessment on such initiatives for the Commissioner's review and comment.

These new oversight powers, along with new requirements for government to consult with the Commissioner on the development of regulations and an information sharing Code of Practice,

have made B.C.'s Information and Privacy Commissioner the most powerful Commissioner in Canada.

Current Context

Elizabeth Denham, who was appointed in May 2010, is British Columbia's third Information and Privacy Commissioner. Prior to her appointment, Ms. Denham served as Assistant Privacy Commissioner of Canada from 2007 to 2010, where she focused primarily on private sector privacy matters.

Ms. Denham has continued to focus on privacy in her current position and has distinguished herself from previous B.C. Commissioners by creating an Assistant Commissioner in charge of a policy and privacy department within her office. This has resulted in a greater involvement in privacy issues and a more detailed review of new initiatives and legislation proposed by government. It has also resulted in the issuance of more public reports on the results of her office's investigations.

This Commissioner uses public statements and the media to a greater extent than her predecessors, a measure that is in line with her stated pursuit of public accountability. She also tends to blend private sector and public sector issues in her public reports and guidelines. This can make implementation challenging as the requirements in the private and public sector privacy acts are different.

The Commissioner's greater focus on privacy, coupled with her earlier and continued involvement in large-scale projects, has increased the number of interactions with her office and brought the importance of government's relationship with the Commissioner to the fore. The Commissioner has a strong mandate to comment on government activity and it is thus important that a positive relationship be fostered.

Current Priorities and Issues

While the Commissioner is generally interested in reviewing and commenting on any large scale program, project or issue, the following themes or topics seem to be of particular interest to her and have been raised by her in multiple forums and contexts:

1. Data-Linking:

S13

S13

S13

2. **Subsidiary Corporations:** The Commissioner has repeatedly called on government to bring subsidiary corporations created by public bodies under the scope of FOIPPA. (They are currently considered to be independent companies and, as such, are not covered). The Commissioner has issued several orders regarding applicants not being able to access records held by subsidiary corporations and she has commented publicly on the inappropriateness of this situation. It is expected that the Commissioner will continue to advocate for this change. The all-party Special Committee that reviewed FOIPPA also recommended that government make this change.

S13

3. **Privacy Management Program (PMP):** The Commissioner has issued recommendations and accompanying guidelines for the private sector on enhancing privacy through the creation of a Privacy Management Program (PMP). As a result of a recent privacy breach investigation, she is now encouraging government to develop a comprehensive PMP based on the principles established for the private sector. It is anticipated that she will formalize her recommendation to government when she releases her public report on the Ministry of Health privacy breach.

S13

S13

- 4. Expanded Privacy Reviews:** During her recent privacy review of Phase 1 of the BC Services Card Project, the Commissioner requested comprehensive security and systems architecture material in order to ensure that the project met the reasonable security requirements in FOIPPA. She also asked to review all communications material. Discussions with her office on this and other matters indicate that a detailed security assessment and the provision of a systems architecture will now be a standard expectation for all future privacy reviews of a proposed project, program or system. This expansion of a privacy impact assessment to include detailed security assessments, architecture documents and, in some cases, communications material, is a new requirement (previous Commissioners have not required this level of detail) that greatly increases the amount of work and time required to consult with the Commissioner on an initiative. Government ministries will be looking for advice and support from OCIO before and during consultation with the Commissioner.
- 5. Duty to Document:** As part of a recent high profile investigation, the Commissioner noted that there was an increase in “oral government” or the practice of not creating written records of decisions or decision-making. In her report, she recommended that government legislate the “duty to document” in FOIPPA, requiring public bodies to create records of any key decisions. This issue was previously raised with the 2010 Special Committee that reviewed FOIPPA but the Committee did not act on this request. In response to the Commissioner’s recommendation, government has suggested that the next Special Committee that reviews FOIPPA may wish to revisit this issue.