Canada

Annual Report on the Administration of the Privacy Act

Shared Services Canada

2011-2012

Table of Contents

Welcome to Shared Services Canada

Shared Services Canada (SSC) was created in August 2011 to fundamentally transform how the Government of Canada manages its information technology (IT) infrastructure. It is mandated to streamline and reduce duplication in the Government's IT infrastructure services while strengthening the security of government and Canadian data. Under this dual mandate, SSC is providing its partner organizations with modern, reliable and secure IT infrastructure services that are cost-effective and which contribute to a greener government. In the process, it is building a new organization from the ground up.

Through SSC, the Government will move to a single email system, consolidate its data centres from over 300 to less than 20 and streamline its electronic networks. SSC will now deliver email, data centre and network services to 43 organizations on a mandatory basis.

The new department will also support the Government's Workplace 2.0 efforts, enabling a more mobile, connected, collaborative and efficient work force. This will improve services to Canadians, make IT more secure and reliable, and save taxpayers' dollars.

Introduction

Privacy Act

Shared Services Canada (SSC) places paramount importance on privacy operations and governance. SSC provides privacy with the purpose, and manner, set forth in the *Privacy Act,* specifically, "to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."

Tabled in Parliament

SSC is pleased to table its first Annual Report to Parliament on the administration of the *Privacy Act* (the Act) for the fiscal year 2011–2012. This Annual report is submitted in accordance with sections 72(1) and 72(2) of the Act.

Departmental Mandate and Priorities

SSC is mandated to simultaneously operate and transform the government's IT infrastructure. Under the umbrella of that dual authority, SSC is responsible for providing its partner organizations with modern, reliable and secure IT infrastructure services that are cost-effective and which contribute to a greener government. In the process, it is building a new organization from the ground up.

SSC has identified the following four priorities for 2012-2013:

1. From an operational perspective, SSC is stabilizing IT service delivery across the Government of Canada. With a focus on business continuity, it is maintaining existing service levels while working to improve them. SSC is supporting a significant number of projects in cooperation with its partners which will both modernize and streamline today's IT operations. This is delivering early results, facilitating SSC's contribution to the government's deficit reduction efforts, and enabling it to plan and build capacity to take on the larger, more complex transformative initiatives.

2. SSC will be launching the renewal of the Government of Canada's IT infrastructure. Working collaboratively with its partners, SSC is identifying an email solution and developing initial plans to consolidate data centres and networks in a whole-of-government approach. Additionally, as a key security services delivery organization, SSC will work collaboratively with other cyber-security agencies to enhance information security across the Government of Canada in order to support the implementation of federal government's new cyber-security strategy.

3. SSC will take advantage of every opportunity to work with partners to fulfill its mandate and realize its objective of improving delivery of services to Canadians in a secure, reliable and integrated manner. Partner departments and agencies have developed many innovative processes, principles and tools over the years and SSC will mine that expertise and leverage best practices. Collaborating and maintaining an open, transparent and meaningful dialogue with industry on IT modernization will also be a critical component of SSC's success. SSC has mapped an engagement process that focuses on developing a sustainable and substantive relationship with the private sector.

4. As a new department, SSC is creating a dynamic corporate culture – one that builds on a broader public service ethos to embrace innovation as part of its brand. Supporting and challenging SSC employees is central to that undertaking. Working together, as a community, SSC will deliver service excellence, innovation and value for money as it builds a modern, reliable and secure IT platform for the Government of Canada.

While SSC employees are currently embedded in 43 partner institutions in order to provide services relating to network infrastructure, email and telecommunications, it is understood that:

- Data housed in SSC-managed servers will be segregated by government institution and access rights will not change.
- The 43 partner institutions are responsible for the creation, maintenance, use, disclosure and disposal of their electronic information holdings.
- From an access to information and privacy (ATIP) perspective, SSC does not have control and ownership over records stored in the shared IT infrastructure.
- Processing ATIP requests of records of the partner institutions remains the responsibility of the respective ATIP Offices.
- The SSC ATIP Office will process only those records under SSC control. However, given the devolution of responsibilities to SSC and thus the shared interest, consultations with the 43 partner institutions will inevitably be a large part of our ATIP process.

Dedicated to ATIP Excellence

When Shared Services Canada (SSC) was created by Order in Council on August 4, 2011, it was also made subject to the *Access to Information Act* and *Privacy Act.* However, during the reporting period 2011-2012, SSC was assisted by Public Works and Government Services Canada (PWGSC) for the processing of requests for records relevant to SSC.

Through a Business Continuity Framework, a cooperative arrangement with partner institutions ensured the continuity of operations while SSC was being established. This Framework also ensured that all corporate, administrative and other support functions continued during the transition, such as for the administration of the *Access to Information Act* and the *Privacy Act* by PWGSC.

While the PWGSC ATIP Office did not process on SSC's behalf any *Privacy Act* requests for access to personal information, it did handle a few Privacy Impact Assessments pertaining to SSC initiatives. For further details see the Statistical Reporting section on page 9.

Delegated Authority

On April 2, 2012, the President of Shared Services Canada delegated full responsibilities under the *Privacy Act* to the Director of the Access to Information and Privacy Protection Division (the ATIP Office) pursuant to section 73 of the Acts. (The SSC Designation Order for the *Privacy Act* is included in Annex A.)

Start-up of SSC ATIP Office

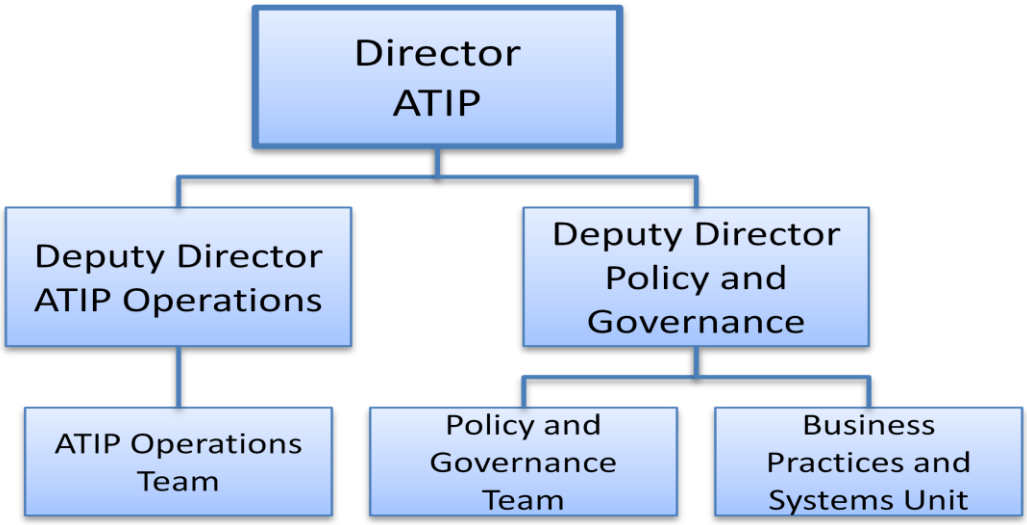
Since April 2012, the SSC ATIP Office has been a stand-alone ATIP Office responding to requests and providing guidance concerning access to information and privacy matters.

With the first order of business completed vis-à-vis the creation of the internal delegation instruments, the second order of business was to establish the ATIP Liaison Officer process which provides a single gateway into each SSC Branch and Directorate in order to streamline the ATIP tasking process. Once the Liaison Officers were identified, the next order of business was to develop and provide hands-on training in order for them to have the necessary knowledge and understanding of their roles and responsibilities to effectively coordinate the ATIP taskings within their respective areas.

The ATIP Office is also actively working on various start-up projects to meet legislative and policy requirements such as publishing the SSC chapter for

Info Source, providing annual ATIP statistical reports to the Treasury Board Secretariat (TBS) and preparing the ATIP Annual Reports to Parliament.

ATIP Office Organizational Chart



The Operations Section within the ATIP Office is responsible for processing requests under the *Access to Information Act* and the *Privacy Act*. This includes liaising with subject-matter experts within SSC, performing a line-by-line review of records requested under the legislation and conducting external consultations as required to balance between Canadians' rights of access and the government's need to safeguard certain information in limited and specific cases. The Operations Section provides briefings for senior departmental officials as required on a case-by-case basis. This Section is also the main point of contact with the Offices of the Information and Privacy Commissioners of Canada with respect to the resolution of complaints pertaining to both Acts.

The Policy and Governance Section provides policy advice and guidance on access to information and the protection of personal information to SSC officials across its Branches and Directorates. This section also prepares and distributes weekly reports on the status of ATIP requests. It is responsible for assisting program officials when they draft personal information sharing agreements and privacy impacts assessments to ensure that the applicable privacy laws are respected. It responds to legal instruments in which the Department is asked to share personal information, (i.e., subpoenas, court orders, search warrants), and liaises with the Office of the Privacy Commissioner on issues such as privacy breaches. It has the privilege of liaising with employees and prepares/delivers training and awareness sessions throughout the Department. The Policy and Governance section coordinates the Department's annual reporting requirements and SSC's input into the TBS annual update of its *Info Source* publication. In addition, this section develops products and tools related to ATIP processing. It provides standards and guidance to the Department on key access to information and privacy issues. It also

has the lead for the TBS Management Accountability Framework lines of evidence 12.4 Access to Information, 12.5 Privacy and 12.6 ATIP Governance and Capacity.

ATIP Training

SSC is building an entire department from the ground up and appreciates the importance of placing emphasis on its people and culture. That is why the ATIP Office is delivering ATIP Liaison Officer training as well as general ATIP Awareness sessions to departmental officials at all levels to ensure that employees are aware of their roles and responsibilities vis-à-vis ATIP compliance.

Underlying Principles for the ATIP Process

The SSC ATIP process is based on best practices within the federal ATIP community which will enable the division to meet the challenges of responding to *Privacy Act* requests in a timely manner.

Similar to the *Access to Information Act* process, the ATIP Office instituted its *Privacy Act* processes based on some of the same principles for duty to assist applicants, which are:

- offer reasonable assistance throughout the request process;
- make every reasonable effort to locate and retrieve the requested records under the control of the institution;
- apply limited and specific exemptions to the requested records;
- provide accurate and complete responses;
- provide timely access;
- provide records in the format and official language requested, as appropriate; and
- provide an appropriate location within the institution to examine the requested information.

The Privacy Principles

SSC also adheres to following privacy principles:

- Accountability: an organization is responsible for personal information under its control.
- Collection: information should be collected fairly, and lawfully; it should be necessary and relevant.
- Consent: the individual must have knowledge to consent for the collection, use or disclosure of personal information, except when appropriate (e.g., lawful investigations).

- Use: personal information is used in line with the purposes of its collection, except when the individual consents, or it is required by law. Personal information is retained only as long as necessary.
- Disclosure: personal information should be disclosed in line with the purpose of its collection, except with an individual's consent or as lawfully required. Personal information is retained only as long as necessary to meet its purpose.
- Accuracy: personal information should be as accurate, complete and up-to-date so as to serve its purpose.
- Safeguards: security safeguards should be appropriate to the sensitivity of the information.
- Openness of information: an organization should make specific information readily available to individuals about its policies, and practices on management of personal information.
- Individual Access: an individual should be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- Challenging Compliance: an individual should be able to address a challenge to compliance.

Control of Records and 43 Partner Institutions

SSC ATIP processes those records that relate to its own internal departmental business. The 43 partner institutions' access rights have not changed and they continue to be responsible for the creation, maintenance, use, disclosure and disposal of their electronic information holdings. (See list of partner institutions under Annex B.)

While SSC does not have control and ownership over institutions' records stored in the shared IT infrastructure, given the devolution of responsibilities and thus the shared interest, consultations with the 43 partner institutions will inevitably be on-going when processing ATIP requests. From an operational perspective, standardized processes will need to be established to avoid inadvertent delays.

Statistical Reporting

Privacy Act Administration in 2011-2012

While the PWGSC ATIP Office did not process on SSC's behalf any *Privacy Act* requests for access to personal information or any consultations it did, during the reporting period 2011-2012, participate in the development of Privacy Impact Assessments pertaining to SSC initiatives. As such, the only tables in the annexed *Privacy Act* statistical report that contain data are 8.1 and 8.2. (See Annex C.)

Resources Related to the Privacy Act

Given that a budget was not allocated to the SSC ATIP Office prior to April 1, 2012, the only amount reported is the actual amount of salary dollars paid in 2011-2012 for two employees joining late in the fiscal year to begin the start-up process. That is, one full-time person worked 2.5 months and a second full-time person worked less than 0.5 months: 2.9 months divided by 12 months/year = 0.24 FTEs. These resources and the associated salary amount of $25,354.54 were used for the administration of both Acts. As such, they are distributed equally between both SSC ATIP annual reports, that is $12,677.00 for each Act.

Complaints and Judicial Reviews

The Department did not receive any complaint notifications from the Office of the Privacy Commissioner in 2011-2012, nor was SSC notified of any applicants asking for judicial review.

Administration of Personal Information

The Privacy Impact Assessment (PIA) Policy that was introduced by TBS in May 2002 was replaced by the April 2010 TBS Directive on Privacy Impact Assessment. This Directive ensures that privacy is taken into account and that privacy implications are appropriately identified, assessed and resolved before a new or substantially modified program, activity or service involving personal information is implemented. It is a step-by-step evaluation of the flow of personal information held within a given program, activity or service.

More specifically, this process enables the Department to determine whether new technologies, information systems, initiatives, and proposed programs, activities, services or policies meet federal government privacy requirements.

Privacy Impact Assessments

During the reporting period 2011-2012 PWGSC initiated, on behalf of SSC, three (3) PIAs relating to:

- Internal Credential Management (MyKey);
- External Credential Management (GCKey/Branded Credential Service); and
- Credential Broker Service, which is part of the Treasury Board Secretariat Cyber Authentication Initiative for the Government of Canada (GC).

Internal Credential Management – Internal to Government, employees will continue to have access to their personal information through online services such as MyKey.

External Credential Management – External to Government, the GCKey/Branded Credential Service will offer the service of issuing, managing and validating anonymous credentials of individuals and businesses accessing and/or communicating with GC systems and applications.

The GC has been offering an online authentication service since 2004. The first service was the e-pass system. In 2009, departments initiated transition projects to migrate away from the e-pass to a new technology called Access Key. This essentially meant that private organizations would continue to provide the primary level of credential services and the GC departments would provide the secondary level of Registration and Authentication.

A PIA of GC Access Key was completed in July 2010 and SSC addressed the recommendations of the Office of the Privacy Commissioner including the establishment of a uniform retention and disposal schedule for personal data and logs related to Access Key. The service is scheduled for termination on December 31, 2012, and thus the introduction of GCKey/Branded Credential Service.

Credential Broker Service – For access to GC services clients will also have a choice to either use the online credentials they already hold with financial institutions through the new Credential Broker Service or they will be able to use the GCKey/ Branded Credential Service.

Personal Information Banks

Effective April 1, 2012, the following three Personal Information Banks were transferred from PWGSC to SSC and will be listed within the Department's first *Info Source* publication under the Program Activity, "Efficient and Effective IT Infrastructure Services":

- Directory Services;
- Internal and External Credential Management Services; and
- Telephone Call Detail Information.

During the reporting period 2012-2013, the ATIP Office will work closely with SSC Information Management to identify all SSC information holdings for the next *Info Source* publication.

Next Steps for the Year Ahead

The ATIP Office appreciates the rare opportunity to be involved in the development of a new organization. It will strive to be innovative in the administration of the *Access to Information Act* and *Privacy Act.* The ATIP Office is committed to supporting the Department as it creates a culture of service excellence and will move towards an efficient and modern paperless environment.

In addition, SSC ATIP will continue to work collaboratively with its 43 partner institutions who are responsible for the creation, maintenance, use, disclosure and disposal of their electronic information holdings. The ATIP Office will develop procedures and implement a standardized ATIP process to ensure a common approach with its partner institutions.

In addition, as part of SSC's Email Transformation Initiative to implement a consolidated and modern email platform, the SSC ATIP Office chairs a Privacy Working Group to make certain that all privacy requirements are addressed.

ANNEXES

ANNEX A: SSC Privacy Act Designation Order

Shared Services Canada / Services partagés Canada

***Privacy Act* Designation Order**

The President of Shared Services Canada, pursuant to section 73 of the *Privacy Act*, hereby designates the persons holding the positions set out in the schedule hereto, or the persons acting in those positions, to exercise the powers and perform the duties and functions of the President of Shared Services Canada as the head of a government institution under all sections of the *Privacy Act*. This designation is effective immediately upon being signed.

SCHEDULE

1. Chief Operating Officer
2. Senior Assistant Deputy Minister and Chief Financial Officer
   Corporate Services
3. Corporate Secretary
4. Director
   Access to Information and Privacy Protection Division

Liseanne Forand

Ottawa, 2.4.12

Canada

ANNEX B: List of Partnership Institutions

1. Aboriginal Affairs and Northern Development Canada
2. Agriculture and Agri-Food Canada
3. Atlantic Canada Opportunities Agency
4. Canada Border Services Agency
5. Canada Economic Development for Quebec Regions
6. Canada Revenue Agency
7. Canada School of Public Service
8. Canadian Food Inspection Agency
9. Canadian Heritage
10. Canadian International Development Agency
11. Canadian Northern Economic Development Agency
12. Canadian Nuclear Safety Commission
13. Canadian Space Agency
14. Citizenship and Immigration Canada
15. Correctional Service Canada
16. Department of Finance Canada
17. Department of Justice Canada
18. Environment Canada
19. Federal Economic Development Agency for Southern Ontario
20. Financial Transactions and Reports Analysis Centre of Canada
21. Fisheries and Oceans Canada
22. Foreign Affairs and International Trade Canada
23. Health Canada
24. Human Resources and Skills Development Canada
25. Immigration and Refugee Board of Canada
26. Industry Canada
27. Infrastructure Canada
28. Library and Archives Canada
29. National Defence
30. National Research Council Canada
31. Natural Resources Canada
32. Parks Canada
33. Privy Council Office
34. Public Health Agency of Canada
35. Public Safety Canada
36. Public Service Commission of Canada
37. Public Works and Government Services Canada
38. Royal Canadian Mounted Police
39. Statistics Canada
40. Transport Canada
41. Treasury Board of Canada Secretariat
42. Veterans Affairs Canada
43. Western Economic Diversification Canada

ANNEX C: Privacy Act Statistical Report Information

Government of Canada / Gouvernement du Canada

Statistical Report on the *Privacy Act*

Name of institution: Shared Services Canada

Reporting period: 8/4/2011 to 3/31/2012

PART 1 – Requests under the *Privacy Act*

	Number of Requests
Received during reporting period	0
Outstanding from previous reporting period	0
Total	0
Closed during reporting period	0
Carried over to next reporting period	0

PART 2 – Requests closed during the reporting period

2.1 Disposition and completion time

Disposition of requests	Completion Time							
	1 to 15 days	16 to 30 days	31 to 60 days	61 to 120 days	121 to 180 days	181 to 365 days	More than 365 days	Total
All disclosed	0	0	0	0	0	0	0	0
Disclosed in part	0	0	0	0	0	0	0	0
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	0	0	0	0	0	0	0	0
Request abandoned	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0

2.2 Exemptions

Section	Number of requests	Section	Number of requests	Section	Number of requests
18(2)	0	22(1)(a)(i)	0	23(a)	0
19(1)(a)	0	22(1)(a)(ii)	0	23(b)	0
19(1)(b)	0	22(1)(a)(iii)	0	24(a)	0
19(1)(c)	0	22(1)(b)	0	24(b)	0
19(1)(d)	0	22(1)(c)	0	25	0
19(1)(e)	0	22(2)	0	26	0
19(1)(f)	0	22.1	0	27	0
20	0	22.2	0	28	0
21	0	22.3	0		

2.3 Exclusions

Section	Number of requests	Section	Number of requests	Section	Number of requests
69(1)(a)	0	70(1)(a)	0	70(1)(d)	0
69(1)(b)	0	70(1)(b)	0	70(1)(e)	0
69.1	0	70(1)(c)	0	70(1)(f)	0
				70.1	0

2.4 Format of information released

Disposition	Paper	Electronic	Other formats
All disclosed	0	0	0
Disclosed in part	0	0	0
Total	0	0	0

2.5 Complexity

2.5.1 Relevant pages processed and disclosed

Disposition of requests	Number of pages processed	Number of pages disclosed	Number of requests
All disclosed	0	0	0
Disclosed in part	0	0	0
All exempted	0	0	0
All excluded	0	0	0
Request abandoned	0	0	0

2.5.2 Relevant pages processed and disclosed by size of requests

Disposition	Less than 100 pages processed		101-500 pages processed		501-1000 pages processed		1001-5000 pages processed		More than 5000 pages processed	
	Number of Requests	Pages disclosed	Number of Requests	Pages disclosed	Number of Requests	Pages disclosed	Number of Requests	Pages disclosed	Number of Requests	Pages disclosed
All disclosed	0	0	0	0	0	0	0	0	0	0
Disclosed in part	0	0	0	0	0	0	0	0	0	0
All exempted	0	0	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0	0	0
Abandoned	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0

2.5.3 Other complexities

Disposition	Consultation required	Legal Advice Sought	Interwoven Information	Other	Total
All disclosed	0	0	0	0	0
Disclosed in part	0	0	0	0	0
All exempted	0	0	0	0	0
All excluded	0	0	0	0	0
Abandoned	0	0	0	0	0
Total	0	0	0	0	0

2.6 Deemed refusals

2.6.1 Reasons for not meeting statutory deadline

Number of requests closed past the statutory deadline	Principal Reason			
	Workload	External consultation	Internal consultation	Other
0	0	0	0	0

2.6.2 Number of days past deadline

Number of days past deadline	Number of requests past deadline where no extension was taken	Number of requests past deadline where an extension was taken	Total
1 to 15 days	0	0	0
16 to 30 days	0	0	0
31 to 60 days	0	0	0
61 to 120 days	0	0	0
121 to 180 days	0	0	0
181 to 365 days	0	0	0
More than 365 days	0	0	0
Total	0	0	0

2.7 Requests for translation

Translation Requests	Accepted	Refused	Total
English to French	0	0	0
French to English	0	0	0
Total	0	0	0

PART 3 – Disclosures under subsection 8(2)

Paragraph 8(2)(e)	Paragraph 8(2)(m)	Total
0	0	0

PART 4 – Requests for correction of personal information and notations

	Number
Requests for correction received	0
Requests for correction accepted	0
Requests for correction refused	0
Notations attached	0

PART 5 – Extensions

5.1 Reasons for extensions and disposition of requests

Disposition of requests where an extension was taken	15(a)(i) Interference with operations	15(a)(ii) Consultation		15(b) Translation or conversion
		Section 70	Other	
All disclosed	0	0	0	0
Disclosed in part	0	0	0	0
All exempted	0	0	0	0
All excluded	0	0	0	0
No records exist	0	0	0	0
Request abandoned	0	0	0	0
Total	0	0	0	0

5.2 Length of extensions

Length of extensions	15(a)(i) Interference with operations	15(a)(ii) Consultation		15(b) Translation purposes
		Section 70	Other	
1 to 15 days	0	0	0	0
16 to 30 days	0	0	0	0
Total	0	0	0	0

PART 6 – Consultations received from other institutions and organizations

6.1 Consultations received from other government institutions and organizations

Consultations	Other government institutions	Number of pages to review	Other organizations	Number of pages to review
Received during the reporting period	0	0	0	0
Outstanding from the previous reporting period	0	0	0	0
Total	0	0	0	0
Closed during the reporting period	0	0	0	0
Pending at the end of the reporting period	0	0	0	0

6.2 Recommendations and completion time for consultations received from other government institutions

Recommendation	Number of days required to complete consultation requests							
	1 to 15 days	16 to 30 days	31 to 60 days	61 to 120 days	121 to 180 days	181 to 365 days	than 365 days	Total
Disclose entirely	0	0	0	0	0	0	0	0
Disclose in part	0	0	0	0	0	0	0	0
Exempt entirely	0	0	0	0	0	0	0	0
Exclude entirely	0	0	0	0	0	0	0	0
Consult other institution	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0

6.3 Recommendations and completion time for consultations received from other organizations

Recommendation	Number of days required to complete consultation requests							
	1 to 15 days	16 to 30 days	31 to 60 days	61 to 120 days	121 to 180 days	181 to 365 days	than 365 days	Total
Disclose entirely	0	0	0	0	0	0	0	0
Disclose in part	0	0	0	0	0	0	0	0
Exempt entirely	0	0	0	0	0	0	0	0
Exclude entirely	0	0	0	0	0	0	0	0
Consult other institution	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0

PART 7 – Completion time of consultations on Cabinet confidences

Number of days	Number of responses received	Number of responses received past deadline
1 to 15	0	0
16 to 30	0	0
31 to 60	0	0
61 to 120	0	0
121 to 180	0	0
181 to 365	0	0
More than 365	0	0
Total	0	0

PART 8 – Resources related to the *Privacy Act*

8.1 Costs

Expenditures		Amount
Salaries		$12,677
Overtime		$0
Goods and Services		$0
• Contracts for privacy impact assessments	$0	
• Professional services contracts	$0	
• Other	$0	
Total		**$12,677**

8.2 Human Resources

Resources	Dedicated full-time	Dedicated part-time	Total
Full-time employees	0.00	0.12	0.12
Part-time and casual employees	0.00	0.00	0.00
Regional staff	0.00	0.00	0.00
Consultants and agency personnel	0.00	0.00	0.00
Students	0.00	0.00	0.00
Total	0.00	0.12	0.12