Service | Innovation | Value

Annual Report to Parliament on the Administration of the *Privacy Act*

2012-2013

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

Welcome to Shared Services Canada

Shared Services Canada (SSC) is a federal department created on August 4, 2011, to fundamentally transform how the Government of Canada manages its information technology (IT) infrastructure.

SSC reports to Parliament through the Minister of Public Works and Government Services and is responsible for delivering mandated email, data centre and network services to its 43 partner departments in a consolidated and standardized manner to support the delivery of Government of Canada programs and services.

The Department also provides certain optional technology related services to government organizations on a cost–recovery basis. With a whole–of–government approach to IT, SSC is creating economies of scale to deliver more efficient, reliable and secure IT infrastructure services to Government of Canada departments.

SSC's mandate was reinforced on June 29, 2012, with the passage by Parliament of the *Shared Services Canada Act*.

Introduction

Privacy Act

The *Privacy Act* came into effect on July 1, 1983. The Act protects the privacy of individuals with respect to their personal information that is held by government institutions, and provides these individuals with a right of access to their information. In addition, the *Privacy Act* gives individuals substantial control over the collection, use and disclosure of their personal information.

Section 72 of the *Privacy Act* requires that the head of every government institution submit an annual report to Parliament, detailing the administration of the Act within the institution for each fiscal year. It is under this provision that this annual report is tabled in Parliament.

This annual report describes how Shared Services Canada (SSC) administered the *Privacy Act* for the period of April 1, 2012, to March 31, 2013.

Departmental Mandate and Organization

Mandate

The Government of Canada created SSC on August 4, 2011, to fundamentally transform how the Government manages its information technology (IT) infrastructure.

SSC reports to Parliament through the Minister of Public Works and Government Services. SSC is mandated to deliver email, data centre and telecommunication services to 43 federal departments and agencies (Partner Organizations). Our department also provides other optional services to government departments and agencies on a cost-recovery basis. The total budget for 2012-2013 was approximately $1.7 billion (including revenue from cost-recovery services).

The creation of SSC brought together people, technology resources and assets from the 43 federal departments and agencies to improve the efficiency, reliability and security of the government's IT infrastructure. A more efficient use of technology will increase productivity across departments and will help build a more modern public service.

SSC’s first priority is to maintain and improve the delivery of IT infrastructure services while renewing the Government's aging IT infrastructure by:

- moving the 43 federal departments and agencies to one consolidated, efficient, secure and modern email system, and consolidating data centres and networks;
- working in partnership with key stakeholders;
- adopting enterprise-wide approaches for managing IT infrastructure services; and
- implementing efficient and effective business management processes in support of its mandate.

Organization

SSC is national in scope, with employees serving 43 government departments and agencies.

Approximately 1,300 IT employees from Public Works and Government Services Canada were transferred to the new department in the summer of 2011. Around 5,000 additional IT and internal services employees from 42 other federal organizations were transferred in November 2011. This experienced workforce operates under a business model (Plan, Build, Operate, Manage) that encourages partnerships and that is based on service excellence, innovation and value for money.

SSC has four branches, each responsible for supporting one of SSC's four pillars:

- Plan and Design – Transformation, Service Strategy and Design Branch
- Build – Projects and Client Relationships Branch
- Operate – Operations Branch
- Management – Corporate Services Branch

Branches are responsible for delivering on the priorities. One of SSC's strengths is the synergies that occur when the various branches work together to deliver IT infrastructure services to SSC's partner organizations.

Delegated Authority

In April, 2012, the President of SSC delegated full responsibilities under the *Privacy Act* to levels down to and including the Director of the Access to Information and Privacy Protection Division (the ATIP Division) pursuant to section 73 of the Act. The SSC Designation Order for the *Privacy Act* is included in Annex A.

Dedicated to Access to Information and Privacy Excellence

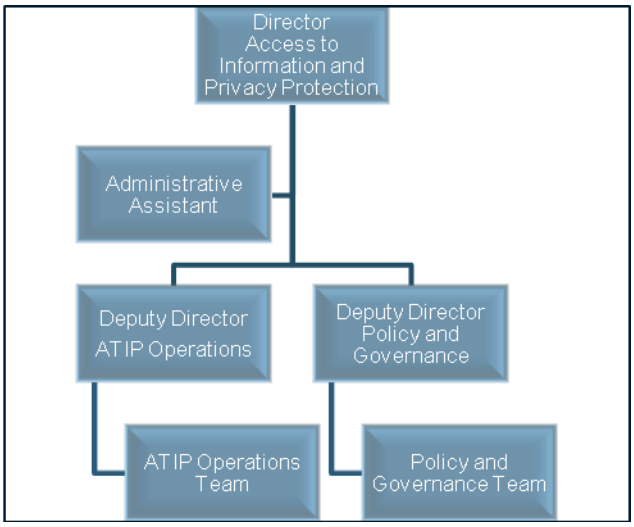
The Director of Access to Information and Privacy (ATIP) Protection is accountable for the development, coordination and implementation of effective ATIP related policies, guidelines, systems and procedures. This accountability ensures that the Department's responsibilities under the *Access to Information Act* and the *Privacy Act* are met, and enables appropriate processing and proper disclosure of information.

The main activities of the ATIP Division include:

- Processing requests under the *Access to Information Act* and *Privacy Act*;
- Developing policies, procedures and guidelines in support of Access and Privacy legislation;
- Promoting awareness of both Acts within the Department to ensure that employees understand their roles and responsibilities;
- Monitoring departmental compliance with both Acts, and maintaining regulations and relevant procedures and policies;
- Preparing annual reports to Parliament and other statutory reports, as well as other material that may be required by central agencies;
- Responding to consultations from other government institutions regarding SSC information under consideration for release;
- Representing the Department in dealings with the Treasury Board of Canada Secretariat (TBS), and the Information and Privacy Commissioners regarding the application of both Acts as they relate to SSC; and
- Supporting the Department in meeting its commitments to openness and transparency through proactive disclosure of information and the release of information via informal avenues.

Access to Information and Privacy Protection Division Structure

The ATIP Division structure has 14 full-time employees (FTEs), and includes the following positions: the Director, two Deputy Directors, one Team Leader, nine analysts, and one support staff. During this first full reporting period, the ATIP Division maintained an average number of 8.9 FTEs, 5.8 of which were dedicated to the administration of the *Access to Information Act*. By the end of the reporting period, the ATIP Division had 11 positions staffed.



The Operations Unit within the ATIP Division is responsible for processing requests under the *Access to Information Act* and the *Privacy Act*. This includes liaising with subject-matter experts within the Department, performing a line-by-line review of records requested under the legislation and conducting external consultations as required to balance between the rights of access and the government's need to safeguard certain information in limited and specific cases. The Operations Unit provides briefings on matters relating to requests and departmental performance for senior departmental officials as required. This unit 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 requests under both Acts.

The Policy and Governance Unit provides policy advice and guidance on access to information and the protection of personal information to departmental officials across its branches and directorates. It is responsible for assisting program officials when they draft personal information sharing agreements and conduct privacy impacts assessments to ensure that privacy legislation is respected. It liaises with employees and prepares and delivers training and awareness sessions throughout the Department. The Policy and Governance Unit coordinates the Department's annual reporting requirements and publishes the SSC *Info Source*[1] chapter in accordance with the TBS *Info Source* Modernization Initiative. In addition, this Unit develops products and tools related to ATIP processing. It provides standards and guidance to the Department on key ATIP issues and it 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. This unit is also the main point of contact with the Offices of the Information and Privacy Commissioners of Canada with respect to the resolution of certain types of complaints pertaining to both Acts, such as systemic investigations and privacy breaches. This same unit also responds to legal instruments, (i.e., subpoenas, court orders and search warrants).

[1] *Info Source: Sources of Government and Employee Information* provides information about the functions, programs, activities and related information holdings of government institutions. The TBS initiated a pilot project to decentralize the publishing of institutional *Info Source* chapters.

Interpretation of the Statistical Report (Annex B)

The TBS Statistical Report on the Administration of the *Privacy Act* provides a summary of the personal information requests and consultations processed during the 2012-13 reporting period.

Overview of Workload

During SSC's second reporting period, the SSC ATIP Division received five requests under the *Privacy Act* and one consultation. Throughout this period SSC has maintained 100% compliance rate on requests, responding within the statutory deadline every time.

SSC has very few program activities involving the collection of personal information from the public. The volume of requests is not expected to increase significantly because of this.

Requests Received under *Privacy Act*

During this reporting period, five requests were received under the *Privacy Act*, four of which were completed before the end of the period.

Disposition of Requests Completed

Of the four completed requests, one request led to the full disclosure of the requested documents, two requests had exemptions applied to parts of the records prior to their release and one request was closed with no relevant records having been located.

Exemptions Invoked

In both requests where some information was withheld, the withheld information related to another individual and was exempted under section 26 of the *Privacy Act*.

Exclusions Cited

No exclusions were invoked in the requests completed during the period.

Completion Time

All of the requests completed in the reporting period were completed within the initial 30 days provided by the Act.

Extension

No extensions were claimed pursuant to section 15 of the Act.

Costs

During the reporting period, the SSC ATIP Division spent $234,678 on salary and $24,721 on goods and services. No overtime was required during the reporting and no professional service contracts were issued.

Personal Information Consultations

During the reporting period, SSC received one consultation from another federal institution. The SSC ATIP office completed the consultation within 15 days.

Access to Information and Privacy Procedures, Policies and Initiatives

As a new ATIP office, the first order of business was the creation of the internal delegation instruments. The second was to establish the ATIP Liaison Officer process which provides a single gateway into each departmental 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 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 for access and consultations in a timely manner.

Similar to the *Access to Information Act* process, the ATIP Division instituted its *Privacy Act* processes based on some of the same principles to assist applicants as defined in the TBS Directive on the Administration of the Access to Information Act:

1. Process requests without regard for the identity of the applicant;
2. Offer reasonable assistance throughout the request process;
3. Provide information about the *Access to Information Act*, including information the process of requests and the right to complain to the Information Commissioner;
4. Inform the applicant as appropriate and without undue delay when the request needs to be clarified;
5. Make every reasonable effort to locate and retrieve the requested records under the control of the institution;
6. Apply limited and specific exemptions to the requested records;
7. Provide accurate and complete responses;
8. Provide timely access;
9. Provide records in the format and official language requested, as appropriate; and
10. Provide an appropriate location within the institution to examine the requested information.

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.

Initial Contact with Requesters

As part of the intake process, the ATIP Operations Team Leader reviews all incoming personal information requests to ensure that they are complete and clear. As appropriate, the requester is contacted and offered the possibility of clarifying the request.

This process provides several benefits. It provides a better service to the requester by reducing the amount of time required to process the clarified request. It is also a more efficient use of departmental resources by eliminating the need to search for, retrieve, review and possibly consult on records that are not desired.

Control of Records and 43 Partner Institutions

During the first few months of the reporting period, the Department became aware of its challenge around clarifying roles and responsibilities regarding the *Privacy Act*. Section 16 of the *Shared Services Canada Act*, which received Royal Assent on June 29, 2012, states that "for the purposes of the *Privacy Act*, the records of other government institutions […] that are, on behalf of those institutions or organizations, contained in or carried on SSC's information technology systems are not under the control of SSC."

Therefore, the ATIP office processes only 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 C.)

In October 2012, the Department communicated this information to its partners by way of an email from the Senior Assistant Deputy Minister (SADM) and Chief Financial Officer, Corporate Services, to the Assistant Deputy Ministers responsible for ATIP for each of the partner organizations. This information was also communicated to the ATIP Coordinators and Chief Information Officers in the 43 partner organizations.

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 organizations is part of SSC's process.

Info Source Modernization Initiative

Info Source: Sources of Government and Employee Information provides information about the functions, programs, activities and related information holdings of government institutions subject to the *Access to Information Act* and the *Privacy Act*. It provides individuals and employees of the government (current and former) with relevant information to access personal information about them held by government institutions subject to the *Privacy Act* and to exercise their rights under the *Privacy Act*.

The TBS initiated a pilot project to decentralize the publishing of institutional *Info Source* chapters. SSC was among the first 32 institutions to publish its own *Info Source* chapter during the reporting period on its own Internet site. The TBS has highlighted the Department's *Info Source* for reference to institutions as a particularly good example.

Access to Information and Privacy Online Requests Initiative

The Government of Canada is modernizing service to Canadians while increasing its open information environment. To improve service quality and ease of access for citizens, and to reduce processing costs for institutions, the Government of Canada is beginning to transform platforms supporting the administration of Access to Information and Privacy. Canadians are allowed, for the first time, to submit and pay for Access to Information requests online with the goal of having this capability available to all departments as soon as feasible.

The Access to Information and Privacy (ATIP) Online Request service was launched on April 9, 2013.

This pilot initiative, which is hosted by Citizenship and Immigration Canada (CIC), allows for ATIP requests to be submitted quickly and efficiently by maximizing online technology. In its initial pilot phase, the Access to Information and Privacy Online Request service allows clients to submit requests and fees online to CIC, SSC and the TBS. Upon the successful implementation of this pilot, the service will be expanded to other federal government institutions.

Given its mandate to fundamentally transform how the Government manages its IT infrastructure, it was natural fit for the Department to participate in the TBS-lead initiative to create an online mechanism to submit ATIP requests online. The process of submitting ATIP requests online is challenged by the need to process the payment of application fees (under the *Access to Information Act*) and need to provide supporting documentation such as proof of consent. Throughout the reporting period, SSC was an active participant in the development of the requirements, the functional model and risk analysis of the pilot project.

Whole of Government Access to Information and Privacy Software Solution

The vast majority of institutions subject to ATIP legislation use specialized file tracking and document redactions systems. The last multi-institutional contract for such systems was awarded in March of 2009 and cannot provide all of the functionalities desired by ATIP practitioners. The TBS has taken the lead in the procurement of a next generation ATIP software solution. This new solution will be offered to all institutions subjects to ATIP legislation throughout the government.

In order to ensure that the requirements for this solution meet the current and future needs of ATIP practitioners, two inter-departmental working groups were established. The first working group is made up of ATIP Coordinators and has recommended the high-level functionalities that would be desired of the new solution. A second working group composed of functional experts or “super users” was setup to break down the high-level requirements into working-level functional requirements.

SSC is represented at both of these working groups and is actively contributing to reshaping the process of ATIP requests.

Breaches, Complaints and Audits

On September 17, 2012, a SSC employee reported that an unencrypted data stick was taken from the workstation. The departmental Chief Information and Security Office conducted a security incident investigation which revealed the following:

- The personal information contained on that data stick was the internal to government Personal Record Identifier of 3,412 of the Department's employees, which had been used by the employee to compile budget information; and
- While the missing USB data stick was never recovered, there has been no indication since then of any attempt to inappropriately use the Personal Record Identifiers.

SSC took the following corrective measures for all personal information to be appropriately handled and safeguarded in order to avoid such incidents in the future:

- On October 5, 2012, the President issued a reminder to all departmental employees regarding their responsibilities when entrusted with sensitive and personal information including safeguards when using USB devices;
- Encrypted USB sticks are now mandatory and a controlled issuance has been put in place along with an upcoming new directive to all employees regarding their use. A departmental Privacy and Security Awareness Strategy (from tools to training) is in development in order to imbed a privacy culture within our newly created institution;
- The Department is also developing an internal Privacy Breach Protocol which will form part of SSC's Privacy Management Framework; and
- The Department will perform regular audits and reviews to detect system or other risks to privacy breaches as per the TBS Policy on Internal Audit.

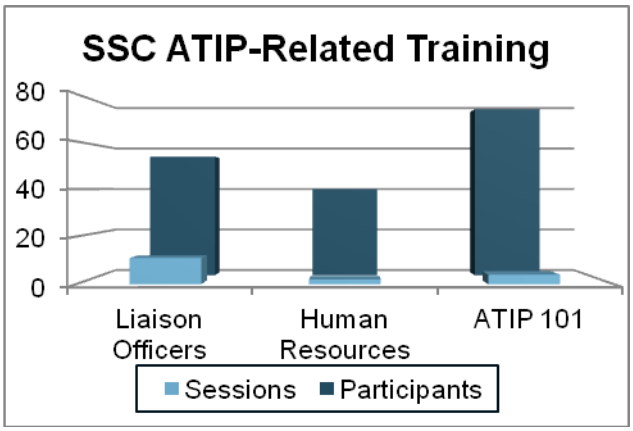
Following SSC's notification to the Office of the Privacy Commissioner, an Incident file was opened and a complaint was subsequently received from one of the affected employees. The Office of the Privacy Commissioner was satisfied with the corrective measures taken by the Department in order to prevent such similar incidents in the future. As such, the Commissioner did not make any recommendations and closed both files as "Early Resolution".

Another unrelated complaint was received concerning the improper collection of personal information. The investigation by the Office of the Privacy Commissioner was ongoing at the end of the reporting period. The result of the investigation will be examined in the next Annual Report to Parliament.

No audits relating to personal information were undertaken or completed during the reporting period.

Departmental Training Activities

During its first year of operation, the SSC ATIP Division focused its efforts on establishing a departmental ATIP process, guiding departmental employees and executives through their requests while maintaining 100% compliance and addressing the training needs of specific areas.



Training for ATIP Liaison Officers

The ATIP Liaison Officer process established by SSC provides a single gateway into each of the branches and directorates in order to streamline the ATIP tasking process. As the primary point of contact for a branch or directorate, the Liaison Officers must have an in-depth understanding of the ATIP process as well as a heightened understanding of the legislation. The ATIP Division developed a three-hour training session and reference material to address the specific needs of the Liaison Officers.

The initial training schedule offered six sessions where 32 Liaison Officers and their backups received the training. An additional five sessions were offered throughout the reporting period as needed to train 23 new Liaison Officers.

ATIP 101

As a start-up organization, the ATIP Division provided various ATIP 101 (general overview) training sessions to departmental officials at all levels. Some of the awareness sessions focused on the internal process for *Access to Information Act* requests and *Privacy Act* obligations in terms of proper personal information handling practices. The Director of ATIP delivered six separate sessions which were attended by a total of 77 departmental officials up to the SADM level.

ATIP Training for Human Resources

Given the nature of the work, the Human Resources and Workplace Directorate approached the ATIP Division for some targeted training for human resources staff. A two-hour training session was developed with a focus on Privacy rights and obligations, including information on Access to Information legislation and the ATIP process. Two such training sessions were delivered to a total of 40 employees.

Departmental Awareness Activities

SSC's Access to Information and Privacy Protection Division and the Security and Information Management Directorate play a key role in managing departmental information holdings. Together, they are developing an integrated approach in fostering awareness, delivering training and providing tools to employees and managers. Integrated awareness initiatives were well received by staff and championed by SSC's senior management.

Launch of the Departmental Website Includes ATIP

This reporting period saw the launch of the departmental website: www.ssc-spc.gc.ca. Access to Information and Privacy content was imbedded into the initial design. The content, including summaries of completed Access to Information Requests, contact information, publications as well as instructions on how to submit an ATIP request and some general information about the ATIP process, met Treasury Board policy requirements on openness, transparency and accessibility.

Right to Know (RTK) Week

Initiated in Bulgaria in 2002, International RTK Week is intended to raise awareness about people's right to access government information while promoting freedom of information as essential to both democracy and good governance. In 2012, the Canadian RTK Week took place from September 24 to September 28. SSC promoted this event by publishing an article on the departmental extranet site.

Security and Protection of Information Communiqué

Public servants are entrusted with sensitive and private information, which we must secure and protect. Departmental employees were reminded of this and their obligations under the *Privacy Act*, *Security of Information Act*, *Access to Information Act*, *Public Servants Disclosure Protection Act*, and *Public Service Employment Act* in a communiqué from the President and the Chief Operating Officer in October 2012.

Data Privacy Day

On January 28, 2013, Canada, along with many countries around the world, celebrated Data Privacy Day. Recognized by privacy professionals, corporations, government officials, academics and students around the world, Data Privacy Day highlights the impact that technology is having on our privacy rights and underlines the importance of valuing and protecting personal information.

SSC promoted this day by a communication across the Department with a message from the Chief Privacy Officer challenging employees to a Privacy Mini-Quiz. This content was well received by public servants with access to the SSC extranet with approximately 4,500 combined page views.

Security Awareness Week

Security Awareness Week is an annual event held the second week of February. It was a success through the continued support of departmental efforts, the Government of Canada security community and inter-departmental groups such as the Security Awareness Working Group.

A departmental working group involving Security, Information Management, Communications and ATIP developed many awareness products for Security Awareness Week, which are featured on the SSC extranet site. Communications also dedicated the February 2013 issue of the Department's monthly newsletter, *iConnect*, to articles by Security and ATIP. The issue featured a message from the SADM and Chief Financial Officer, Corporate Services, concerning appropriate use and disclosure of information as priority for SSC and central to the Department's commitment to Canadians and our 43 partner organizations who place their trust in us every day.

Privacy Impact Assessments

During the reporting period, the department completed three Privacy Impact Assessments and these Summaries are posted on the SSC Internet site: Publications – Access to Information and Privacy.

GCKey – Government Branded Credential Service

The goal of Cyber Authentication Renewal was to provide end-users choice in the credentials they use to authenticate online to Government of Canada programs and services and to provide Government of Canada departments and agencies with the flexibility to determine authentication solutions commensurate with the security needs of their programs and services.

The GCKey system is used to issue, manage and validate anonymous credentials for individuals that wish to make use of Government of Canada Online Services.

The personal information that is collected and used for registering and managing GCKey will be described in the new Personal Information Bank PCU 607 External Credential Management. The personal information may include username, password, password recovery questions and responses, Persistent Anonymous Identifier or Meaningless But Unique Number and Internet Protocol address.

SecureKey Concierge - Credential Broker Service

The Credential Broker Service is an anonymous authentication service which protects privacy. SecureKey Concierge allows end-users to access Government of Canada online services using credentials they already hold with financial institutions. Through the implementation of this commercial service in the spring of 2012, the Government of Canada is able to leverage the considerable industry investment taking place in cyber authentication technology. This is providing individuals with a client-centric, secure online credential authentication solution at a significantly reduced cost to the Crown.

The personal information collected by the Broker has no contextual sensitivities and is never combined with identifying information about the user. In addition, the identifiers, such as, the Name and Recovery Question that the Department or Agency holds, which form part of the Authentication Request, are not disclosed to a Bank.

Access to Information and Privacy (ATIP) Online Requests

This Privacy Impact Assessment is a tri-institutional initiative for Access to Information and Privacy Online Request service. This service provides an e-requesting platform which enables this new electronic request process, thereby eliminating the need to send and receive requests and fee payments by mail. The scope of this Privacy Impact Assessment encompasses the electronic collection of personal information while re-examining the collection, use, disclosure and retention within the interoperability of this single window e-request service. This Assessment covers the data flow of the information through the system, from the point of collection by CIC to the point of reception of the request by the appropriate ATIP Office of the three participating institutions. The TBS coordinated the production of the Privacy Impact Assessment and submitted it to the Office of the Privacy Commissioner on behalf of all participating institutions.

Disclosure of Personal Information Pursuant to Paragraph 8(2)(m)

Paragraph 8(2)(m) of the *Privacy Act* allows the Head of the institution to disclose personal information in cases where the public interest clearly outweighs the invasion of privacy of the individual or when it is clearly in the best interest of the individual. SSC made no disclosures of personal information under this provision.

Next Steps for the Year Ahead

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

During the next reporting period, SSC's ATIP Division will endeavour to improve the internal ATIP process. To accomplish this, the ATIP Division will build on the ATIP process mapping exercise and will undertake a cyclical review of the ATIP process by way of a survey to departmental ATIP Liaison Officers and subsequent consultations. Also, the ATIP Division will launch a resource website for employees on the departmental extranet site and finalize ATIP Guidelines for ATIP Analysts. This will ensure a consistent approach in the processing of Access to Information requests.

A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information. The ATIP Division is developing and implementing a Privacy Breach Protocol which will include reporting and notification tools to assist in responding to all privacy breach situations. Many will be leveraged against tools developed by the federal ATIP Community and align with the TBS Guidelines on Privacy Breaches.

In addition, the ATIP Division will develop a Privacy Management Framework to ensure that personal information collected, used, retained, and disclosed by SSC reflects the Department's responsibilities under the *Privacy Act* and provides a comprehensive governance and accountability framework. The Framework will explain how SSC is organized through structures, policies, systems and procedures to manage privacy risks, distribute privacy responsibilities, coordinate privacy work, and ensure compliance with the *Privacy Act*, *Access to Information Act*, related TBS policies and directives as well as internal departmental policies such as the internal Privacy Breach Protocol. Also, protection of personal information will be ensured through a default system control mechanism. This is currently under development by the departmental Transformation, Service Strategy and Design Branch and is being reviewed in collaboration with an interdepartmental ATIP working group, chaired by the SSC's ATIP Division.

In addition, the ATIP Division continues to work with the Information Management Division as the Department implements a strategy for the formal transfer of records from the 43 partner organizations into its own information holdings. This collaborative initiative will define the Department's information holdings to provide clarity to its *Info Source* chapter and assist requesters in addressing their requests to the proper institution. The results of this initiative will be communicated to partner organizations through continued communication at the senior management level and with departmental ATIP Coordinators. The ATIP Division assists in this endeavour through such forums as the ATIP Community meetings, coordinated by the TBS, to share and discuss with colleagues SSC's role concerning custody and control of records across the Government of Canada.

In collaboration with the departmental Information Management, Security, ATIP, Human Resources and Communications directorates, an integrated work plan was developed and a series of activities, designed to engage employees, are being implemented. The results will inform the development of a departmental SSC integrated training plan for privacy and access, security and IT security as well as information management.

Annex A – Delegation 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 –Statistical Report on the *Privacy Act*

Government of Canada / Gouvernement du Canada

Statistical Report on the *Privacy Act*

Name of institution: Shared Services Canada

Reporting period: 04/01/2012 to 03/31/2013

PART 1 – Requests under the *Privacy Act*

	Number of Requests
Received during reporting period	5
Outstanding from previous reporting period	0
Total	5
Closed during reporting period	4
Carried over to next reporting period	1

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	1	0	0	0	0	0	0	1
Disclosed in part	0	2	0	0	0	0	0	2
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	1	0	0	0	0	0	0	1
Request abandoned	0	0	0	0	0	0	0	0
Total	2	2	0	0	0	0	0	4

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	2
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	1	0	0
Disclosed in part	2	0	0
Total	3	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	34	34	1
Disclosed in part	843	516	2
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	1	34	0	0	0	0	0	0	0	0
Disclosed in part	1	31	0	0	1	485	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	2	65	0	0	1	485	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	1	1	0	0
Outstanding from the previous reporting period	0	0	0	0
Total	1	1	0	0
Closed during the reporting period	1	1	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	1	0	0	0	0	0	0	1
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	1	0	0	0	0	0	0	1

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		$234,678
Overtime		$0
Goods and Services		$24,721
• Contracts for privacy impact assessments	$0	
• Professional services contracts	$0	
• Other	$24,721	
Total		$259,399

8.2 Human Resources

Resources	Dedicated full-time	Dedicated part-time	Total
Full-time employees	0.00	2.46	2.46
Part-time and casual employees	0.00	0.04	0.04
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	2.50	2.50

Annex C – 43 Partner Organizations

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