Service | Innovation | Value

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

2015–2016

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

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 held by government institutions. It establishes the rules for the collection, use, disclosure, retention and disposal of such information. It also provides individuals with a right to be given access to, and to request a correction of, their personal information.

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

The present annual report describes how Shared Services Canada (SSC) administered the *Privacy Act* for the period from April 1, 2015 to March 31, 2016.

Institutional Mandate and Organization

Mandate

SSC was created on August 4, 2011 to transform how the Government of Canada manages its information technology (IT) infrastructure. SSC delivers email, data centre, network and workplace technology device services to departments and agencies in a consolidated and standardized manner to support the delivery of Government of Canada programs and services. With a whole-of-government approach to IT infrastructure services, SSC is generating economies of scale to deliver more efficient, reliable and secure IT infrastructure services. SSC also provides certain optional technology services to other organizations on a cost-recovery basis.

The *Shared Services Canada Act* recognizes that the Government of Canada wishes to standardize and streamline, within a single shared services entity, certain administrative services that support government institutions. Through Orders-in-Council, the Department received specific responsibilities in the area of IT infrastructure services.

SSC's focus is to maintain and improve IT service delivery across the Government of Canada, enhance security and implement government-wide solutions to transform IT infrastructure in order to improve value for money and services to Canadians. The Department works closely with its partner organizations (see Annex A), other government clients, industry and the IT community across Canada.

SSC contributes to the achievement of other critically important Government of Canada initiatives, including border security, benefit payments and weather forecasting, as well as the vision of the future public service as articulated in Blueprint 2020. In addition, SSC works collaboratively with Government of Canada cyber security agencies to improve cyber and IT security.

As of September 1, 2015, Order-in-Council 2015-1071 provides SSC with the authority to offer any or all of its services to any federal government entity on a voluntary basis, as well as to another Canadian jurisdiction or a foreign government, as long as there are no additional costs incurred or additional resources allocated by SSC. The Order-in-Council also expands the mandatory nature of a sub-set of SSC services related to email, data centres and networks to a range of new clients. Most small departments and agencies previously not served, or served only on an optional basis, are set out as mandatory clients for this sub-set of services.

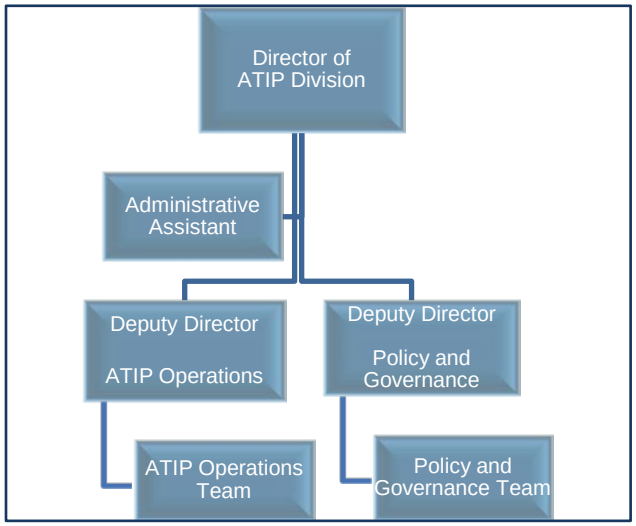
Organization: The way forward

As SSC evolves to execute its Transformation Plan, a new organizational structure has helped shift the Department's focus from its legacy environment to its new enterprise IT infrastructure. On April 1, 2015, SSC moved to a structure where single operational branches are responsible for the entire lifecycle of the services they provide. A flatter, streamlined and more horizontal structure has enabled these goals by clarifying accountabilities on major initiatives and supporting employee mobility.

Delegated Authority

With the arrival of a new President for SSC, pursuant to section 73 of the *Privacy Act*, in August 2015 the President authorized the delegation instrument by reconfirming full powers, duties and functions under the Act to levels down to and including the Director of the Access to Information and Privacy (ATIP) Protection Division, hereafter referred to as the ATIP Division (see Annex B).

ATIP Division Structure



During the reporting period, the ATIP Division structure remained the same with a Director and two Deputy Directors, each overseeing teams of analysts for the Operations side as well the Policy and Governance side. While an average of 16 person years were dedicated to the ATIP program, five person years were dedicated to the administration of the *Privacy Act*. These person years include full-time equivalents, casual employees, students and consultants.

The Operations Unit within the ATIP Division is responsible for processing requests under the *Privacy Act* and its accompanying piece of legislation, the *Access to Information Act*. This includes liaising with subject-matter experts within SSC, performing a line-by-line review of records requested and conducting external consultations as required to balance the public's right of access and the government's need to safeguard certain information in limited and specific cases. The Operations Unit provides briefings for the senior management team as required on matters relating to requests and institutional performance. This unit is also the main point of contact with the Offices of the Privacy and Information Commissioners of Canada with respect to the resolution of complaints related to requests under both Acts.

The Policy and Governance Unit within the ATIP Division provides policy advice and guidance to SSC's senior management team on access to information and the protection of personal information. This unit also develops ATIP policy instruments, processing products and tools. It is responsible for assisting program officials when they conduct privacy impact assessments (PIA) and draft personal information-sharing agreements to ensure that privacy legislation and policy requirements are respected. It also liaises with employees and prepares and delivers training and awareness sessions throughout SSC. In addition, the unit co-ordinates SSC's annual reporting requirements and publishes SSC's *Info Source* chapter.[1] Lastly, it is the main point of contact with the Offices of the Privacy and Information Commissioners of Canada with respect to various audits, reviews, systemic investigations and privacy breaches.

[1] *Info Source: Sources of Federal Government and Employee Information* provides information about the functions, programs, activities and related information holdings of government institutions. Pursuant to the Treasury Board of Canada Secretariat's *Info Source Decentralized Publishing Requirements*, institutions must update their own *Info Source* chapter annually and publish the updated version on their anniversary. SSC's reporting month is June.

Dedicated to ATIP Excellence

The ATIP Division is responsible for developing, co-ordinating, implementing and monitoring compliance with effective ATIP-related policies, guidelines, systems and procedures across SSC. This enables SSC to meet the requirements and to fulfill its obligations under the *Privacy Act* and its accompanying piece of legislation, the *Access to Information Act*.

The main activities of the ATIP Division are:

- Receiving, co-ordinating and processing requests under the *Privacy Act* and the *Access to Information Act*;
- Responding to consultations from other government institutions regarding SSC information under consideration for release;
- Developing and maintaining SSC-specific policy instruments in support of access and privacy legislation;
- Developing and delivering ATIP awareness and training across SSC so that employees and management understand their roles and responsibilities;
- Supporting a network of ATIP Liaison Officers across SSC who assist with requests by co-ordinating the retrieval of records and recommendations from within their branch or region;
- Monitoring institutional compliance with both Acts and their regulations, as well as relevant procedures and policies;
- Preparing annual reports to Parliament on the administration of the Acts, as well as other material that may be required by central agencies;
- Representing SSC in dealings with the Treasury Board of Canada Secretariat (TBS), and the Offices of the Privacy and Information Commissioners of Canada regarding the application of both Acts as they relate to SSC;
- Supporting SSC in meeting its commitments to openness and transparency through the proactive disclosure of information and the release of information via informal avenues, such as the Open Government portal;
- Supporting the Corporate Secretariat's Business Process Transformation by simplifying the Access to Information request process to ensure timeliness and quality review of the information;
- Monitoring ATIP tasking performance and reporting to senior management on a monthly basis; and
- Participating in whole-of-government initiatives for the federal ATIP community.

Interpretation of the Statistical Report – Requests for Personal Information and Consultations

The Statistical Report (Annex C) on the *Privacy Act* provides a summary of the personal information requests and consultations processed during the 2015–2016 reporting period.

Overview of Workload (Annex C, Parts 1 and 2, Table 2.5.1, Table 2.6.2)

During the reporting period, the ATIP Division received 123 requests under the *Privacy Act*. There were no consultations under the *Privacy Act* from other government institutions and there were no requests carried forward from the previous reporting period. The ATIP Division processed a total of 120 requests and carried over three *Privacy Act* requests to the next reporting year.

While the number of requests received under the *Privacy Act* during this reporting period almost doubled compared to the previous reporting period (in which 71 requests had been received), many requests were misdirected to SSC. Out of 6,268 pages processed by the ATIP Division, 3,354 pages were deemed relevant to the *Privacy Act* requests and either disclosed in whole or in part.

The ATIP Division closely tracks, on a weekly basis, its turnaround times in processing requests and monitors the timeliness of their completion. In this reporting period, all processed *Privacy Act* requests were completed within legislated timelines.

Requests Received (Annex C, Parts 1)

During the reporting period, 123 requests were received under the *Privacy Act*. No requests from the previous reporting period were carried forward, for a total of 123 requests requiring action for this reporting period.

Disposition of Requests Completed (Annex C, Part 2, Table 2.1)

Before the end of the reporting period, 120 requests were completed. Of these requests, four led to the full disclosure of the requested documents, 22 had exemptions applied to parts of the records prior to their release, and none had exemptions applied to the records in their entirety. There were no records that existed for 76 requests for various reasons but primarily because of misdirected online requests, and 18 requests were abandoned by the requesters.

Completion Time (Annex C, Part 2, Table 2.1)

The *Privacy Act* sets the timelines for responding to privacy requests. It also provides for extensions in cases where responding to the request within the original time limit would unreasonably interfere with the operations of the government institution or where consultations are necessary but cannot reasonably be completed within the original time limit. Of the 120 requests, 104 (87%) were completed by the 30-day deadline established by the Act. The remaining 16 requests were completed within the lawful time extension of 30 additional days.

Exemptions Invoked (Annex C, Part 2, Table 2.2)

The *Privacy Act* allows, and in some instances requires, that some personal information be exempted and not released. For example, personal information may be exempted when it relates to law enforcement investigations or another individual besides the requester, or when it is subject to solicitor-client privilege.

During the reporting period, there were 22 instances where some information was withheld because it related to another individual and was therefore exempted under section 26 of the *Privacy Act*.

There were three instances where some information was exempted because it related to solicitor-client privilege and was therefore exempted under section 27 of the *Privacy Act*.

Exclusions Cited (Annex C, Part 2, Table 2.3)

The *Privacy Act* does not apply to information that is already publicly available, such as government publications and material in libraries and museums. It also excludes material such as Cabinet confidences. There were no exclusions cited in the requests completed during the reporting period.

Disclosure of Personal Information Pursuant to Paragraphs 8(2)(e) and (m) (Annex C, Part 3)

Paragraph 8(2)(*e*) of the *Privacy Act* allows the head of the institution to disclose personal information without the consent of the affected individual where such information is requested in writing by a designated investigative body for law enforcement purposes. During the reporting period, SSC made no disclosures of personal information under this provision.

Paragraph 8(2)(*m*) of the *Privacy Act* allows the head of the institution to disclose personal information without the consent of the affected individual in cases where, in the opinion of the head, the public interest outweighs any invasion of privacy that could result from the disclosure or when it is clearly in the best interest of the individual to disclose. During the reporting period, SSC made no disclosures of personal information under this provision.

Subsection 8(5) of the *Privacy Act* obliges the head of the institution to notify the Office of the Privacy Commissioner of Canada prior to, or if not practical, forthwith on, any disclosure under paragraph 8(2)(m). SSC made no disclosures of personal information under this provision. Therefore, no notifications to the Privacy Commissioner's office were required under subsection 8(5) of the Act.

Extensions (Annex C, Part 5, Table 5.1)

Extensions permissible under section 15 of the *Privacy Act* were claimed for 16 requests. In 15 of the 16 cases, the extensions were sought for 30 additional days because of the requirement to review large volumes of information, and for the final case, SSC needed to consult another department.

Consultations (Annex C, Part 6)

During the reporting period, SSC received no consultations under the *Privacy Act* from other government institutions.

Costs (Annex C, Part 10)

According to the information provided by SSC's Finance Division in April 2016, during the reporting period, the ATIP Division spent for the administration of the *Privacy Act* a total of $411,699, of which $367,516 was spent on salaries, including $73.00 in overtime, and $44,183 was spent on goods and services, including professional service contracts.

Institutional ATIP Training and Awareness Activities

The ATIP Division continued its efforts toward embedding a culture of ATIP excellence across SSC. It focused on delivering training and awareness activities. In order to assess and continuously improve the effectiveness of its training activities, the ATIP Division uses a comprehensive evaluation form for participants to provide feedback regarding their training experience. During the reporting period, the ATIP office developed a Directive and Standard on the delivery of ATIP training and awareness activities that, among other things, requires the ATIP office to follow up with participants three and six months following the session to gage the retention of the information that was presented. At the end of this reporting period, the ATIP office was working on elaborating such performance indicators.

A total of 14 ATIP training and awareness sessions were delivered to over 400 participants, which included SSC executives, managers and employees at various levels.

Training for the ATIP Liaison Officer Network

As the primary point of contact for a branch or directorate, an ATIP Liaison Officer must have an in-depth understanding of the ATIP process and 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 ATIP Liaison Officers. During the reporting period, the ATIP office delivered four sessions to ATIP Liaison Officers and their delegates for a total of 263 participants.

ATIP Training for Subject-Matter Experts in Offices of Primary Interest

Several program areas requested training on the ATIP process and the nature of exemptions. A three-hour ATIP training program was developed with a focus on the legislative context, SSC's internal process and best practices for responding to ATIP requests. During the reporting period, the ATIP office delivered one general Office of Primary Interest (OPI) training session and eight OPI training sessions to specific groups: one for the Procurement and Vendor Relationships group, one for the Networks and End User group, two for the Human Resources and Workplace group, two for the Data Centre Services' Project Management group, one session for the new Assistant Deputy Minister (ADM) of Service Delivery and Management group and one session to the "learn iT" group regarding the Standard on Managing Privacy Breaches.

The ATIP office has also conducted awareness sessions regarding privacy breaches to groups such as the Account Executives Team, the Service Delivery Management Team and the TBS-led Chief Information Officer Council. These sessions were very well attended and well received by the participants.

ATIP in the Government of Canada

The Director of SSC's ATIP Division also delivered, for the Canada School of Public Service, the three-day ATIP course entitled "Access to Information and Privacy in the Government of Canada" (Course I703), which is intended for federal public servants.

Right to Know Week

In 2015, the Canadian Right to Know (RTK) Week took place from September 28 to October 2. Initiated in Bulgaria on September 28, 2002, International Right to Know Day is intended to raise awareness about people's right to access government information while promoting freedom of information as an essential feature of both democracy and good governance. SSC promoted RTK Week by highlighting it in its weekly bulletin to employees as an awareness campaign that encouraged employees to participate in an online quiz on the SSC extranet site.

Data Privacy Day

On January 28, 2016, 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 issuing a communiqué to employees from the Chief Privacy Officer highlighting that public servants are required to act with integrity and in a manner that will bear the closest public scrutiny. The Chief Privacy Officer also encouraged all SSC employees to consult the SSC Standard on the Code of Privacy Principles.

The Data Privacy Day content is available to public servants on the Department's *MY SSC* extranet site.

ATIP Awareness for SSC Networks

The ATIP Division collaborated with the SSC Managers Network and the Administrative Professionals Network to promote awareness. In December 2015, a message was sent to all SSC managers informing them of SSC's ATIP Internal Policy Instruments and the important role they play in meeting the rights of access to information as well as the protection of personal information. Additionally, in September 2015, the ATIP office delivered an ATIP 101 Webinar session to the Administrative Professionals Network in which 595 individuals participated.

ATIP Policy Instruments, Procedures and Initiatives

As a new initiative during the reporting period, in July 2015, a new tasking and approval process was implemented department-wide based on the ATIP request's level of risk to SSC. The Corporate Secretariat's RACI model (Recommend, Approve, Consult, Inform) is meant to designate the appropriate branch approval level when reviewing ATIP taskings. Requests that are seen as low to moderate risk are tasked and approved at the directorate level (Director General/Senior Director) and requests deemed high risk are tasked and approved at the branch level (ADM). However, ADMs are still informed on all ATIP taskings involving their branch regardless of the level of risk. This new tasking and approval model at the directorate and branch level has proven to be effective in significantly improving the response time of OPIs.

In addition, during this reporting period, SSC continued to work toward embedding a culture of access and privacy excellence. The Department updated the inventory of its information holdings in *Info Source* vis-à-vis its 2014–2015 Program Alignment Architecture. Also during this year, ATIP weaved privacy controls into the departmental Functional Direction document, which is published on the SSC *SERVING GOVERNMENT* website.

ATIP Management Framework

During the reporting period, the ATIP Division updated its ATIP Management Framework, which sets out a comprehensive governance and accountability structure. This Framework reflects SSC's responsibilities under both the *Privacy Act* and the *Access to Information Act* with respect to access rights and with regard to SSC's collection, use, disclosure, retention and disposal of personal information.

In 2015–2016, several policy instruments were approved, implemented, posted on SSC's extranet site and communicated to employees via a Communiqué from SSC's President and Chief Privacy Officer. These policy instruments explain how SSC is organized in terms of its policies and procedures for, among other things, responding to access requests, managing privacy risks, assigning privacy responsibilities, co-ordinating privacy work and ensuring compliance with the *Privacy Act*, the *Access to Information Act*, related TBS policies and directives, and internal SSC policies. These ATIP policies also outline SSC's ongoing efforts to promote ATIP learning and awareness as well as ensuring that all SSC employees, regardless of level, are aware of their responsibilities and obligations under both the *Privacy Act* and the *Access to Information Act*.

The following ATIP policy instruments with tools were approved by the Corporate Management Board and published on SSC's website during the reporting period:

- **Directive on Access to Information and Privacy Training and Awareness with companion**
    - **Standard on the Delivery of Access to Information and Privacy Training and Awareness** – supports SSC in embedding ATIP excellence through training and awareness.
- **Directive on Monitoring Access to Information and Privacy Compliance** – supports SSC in monitoring, for compliance with the *Privacy Act* and the *Access to Information Act*, specific internal

policy instruments designed to manage privacy risks and foster access to records containing information, including personal information, under SSC's control.

- **Standard on Preventing and Managing Obstruction to the Right of Access** – establishes the procedures for addressing instances of perceived or actual obstruction of lawful access to information under SSC's control.

- **Directive on Conducting Privacy Impact Assessments** – supports SSC in meeting its obligations to manage privacy risks and in project-management excellence.

  - **Standard on the Use of Personal Information for Non-Administrative Purposes** – provides comprehensive governance and accountability in activities involving the collection, use or disclosure of personal information for non-administrative purposes with companion SSC Social Media Privacy Checklist, which determines if a PIA is required or whether an amendment to an existing PIA must be completed because of potential privacy risks with the proposed social media activity.

  - **Standard on the Code of Privacy Principles** – ensures that every reasonable measure is taken to reduce potential risks of privacy breaches.

In addition, the following five new policy instruments, which were approved by the Corporate Management Board in March 2016, will be published on SSC's website in the next reporting period:

- **Directive on Managing Personal Information Required for Administrative Purposes and Lawful Investigations** – supports SSC's commitment in establishing and adhering to best practices for collecting, retaining, using, disclosing and disposing of personal information in strict compliance with the *Privacy Act*.

  - **Standard on Facilitating Access to Data Under the Control of Partner Organizations** – supports timely and effective service to SSC's partners whose data resides on SSC's IT infrastructure. This Standard provides comprehensive governance and accountability in facilitating partner access to their data.

  - **Standard on the Use and Disclosure of Personal Information Under the Control of SSC** – supports effective privacy management at SSC by providing comprehensive governance and accountability in SSC's use and disclosure of personal information under its control.

  - **Standard on eDiscovery Multi-Mailbox Searches for Access to Information and Privacy Purposes** – supports access to information and privacy management at SSC by providing comprehensive governance and accountability involving the use of MMS/eDiscovery activities warranted by an ATIP request.

- **Standard on Managing Personal Information in Emergencies** – supports effective privacy management at SSC by providing comprehensive direction in activities involving the handling of personal information under SSC's control in the event of an emergency.

"Duty to Assist" Principle

The ATIP Division's process under the *Privacy Act* is based upon the "duty to assist" principle, which is defined in the TBS Directive on Privacy Requests and Correction of Personal Information as follows:

1. Process requests without regard for the identity of the applicant;
2. Offer reasonable assistance throughout the request process;
3. Provide information on the *Privacy Act*, including information on the processing of requests and the right to complain to the Privacy Commissioner of Canada;
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 personal information under the control of the institution;
6. Apply limited and specific exemptions to the requested personal information;
7. Provide accurate and complete responses;
8. Provide timely access to the requested personal information;
9. Provide personal information in the format and official language requested, as appropriate; and
10. Provide an appropriate location within the institution to examine the requested personal information.

SSC's ATIP process is further supported by best practices within the federal ATIP community, which enable SSC to meet the challenges of responding in a timely manner to *Privacy Act* requests for access and consultations.

SSC also adheres to the following privacy principles:

- Accountability – an institution is responsible for personal information under its control.
- Purposes – the purposes for which personal information is collected shall be identified at or before the time the information is collected.
- Collection – information should be collected fairly and lawfully and should be necessary and relevant.
- Consent – the individual must have knowledge of the collection, use or disclosure of personal information in order to be able to consent to it, except when inappropriate (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.
- Disclosure – personal information should be disclosed in line with the purpose of its collection, except when the individual consents or it is required by law.
- Retention – personal information is retained only as long as necessary.
- Accuracy – personal information should be 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 institution should make specific information readily available to individuals about its policies and practices on the management of personal information.

- Individual access – an individual should be able to access his or her personal information under the control of the institution.
- Challenging compliance – an individual should be able to challenge compliance with any of the above principles by contacting the ATIP Division and/or the Privacy Commissioner of Canada.

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 clearly determining the scope of the requested information, thereby potentially reducing the processing time. It also makes more efficient use of institutional resources by eliminating the need to search for, retrieve, review and possibly consult on records that are not desired.

ATIP Process Manual

During the reporting period, the ATIP Division continued to update its procedural manual to guide ATIP staff in processing requests received under the *Privacy Act* and its accompanying piece of legislation, the *Access to Information Act*. The manual provides information about the types of documents processed and how they should be handled pursuant to the Acts. The manual serves as a reference tool for ATIP staff and is designed to ensure consistent application of the Acts and related policy instruments. Further, the manual supports SSC's "duty to assist" all applicants, so that all reasonable effort is made to help applicants receive complete, accurate and timely responses in accordance with the legislation.

SSC has developed internal procedures and guidelines to ensure appropriate monitoring of and reporting on ATIP requests, as well as compliance with TBS policies and guidelines. They provide important checks and balances required to maintain full compliance.

Cabinet Confidence Process

SSC's ATIP Division has a Service Level Agreement with its institutional Legal Services Unit for the provision of a review and recommendations on records that may contain information subject to the Cabinet confidences exclusion. This Service Level Agreement allows for an efficient business process related to Cabinet confidences, thereby ensuring that SSC meets the requirements of the revised process and fulfills its obligations under the *Privacy Act*.

Control of Records and Partner Organizations

Given SSC's mandate, there are challenges surrounding the roles and responsibilities under the *Privacy Act*. Section 16 of the *Shared Services Canada Act* states that:

> …for the purposes of the *Privacy Act*, personal information that is collected by other government institutions as defined in that Act or by other organizations and that is, on behalf of those institutions or

organizations, contained in or carried on Shared Services Canada's information technology systems is not under the control of Shared Services Canada.

The ATIP Division processes only those records that relate to SSC departmental business. The partner organizations continue to be responsible for the creation, maintenance, use, disclosure and disposal of their electronic information holdings, and their access rights have not changed.

While SSC does not have control and ownership over the partner organizations' records stored in the shared IT infrastructure, given the responsibilities and thus the shared interest, consultations with the partner organizations (see Annex A) is an important part of SSC's processing of requests.

Partner organizations may from time to time require SSC's assistance to access their data residing on the SSC IT infrastructure. SSC's Security Operations Centre (SOC) is instrumental in the new process and is the primary contact within SSC to facilitate partner access to their data when all efforts by partners to retrieve such records internally have been unsuccessful. This would be the case in three different scenarios:

1. when partners receive ATIP requests for their records (records under their control residing on the SSC IT infrastructure);
2. when partners are subject to court orders, subpoenas, warrants or any other binding order made by a person or body with jurisdiction to compel the production of records; and
3. when a lawful investigation (administrative or criminal) requires the retrieval of records residing on the SSC IT infrastructure.

***Info Source* Update**

Info Source: Sources of Federal Government and Employee Information provides information about the functions, programs, activities and related information holdings of government institutions subject to the *Privacy Act* and the *Access to Information Act*. It provides individuals as well as current and former employees of the government with relevant information to assist them in accessing personal information about them held by government institutions subject to the *Privacy Act* and exercising their rights under the *Privacy Act*.

TBS requires that government institutions publish their own *Info Source* chapter on their Internet site. During the reporting period, SSC completed its review of its *Info Source* chapter and met all legislative and TBS mandatory requirements.

ATIP Online – Recognition Award

On May 21, 2015, the SSC ATIP Division was recognized at the IM-IT Community Recognition Awards for its participation in the pilot for the ATIP Online Request Service. The awards are administered by the Service and GC2.0 Policy and Community Enablement Division of TBS, on behalf of the Access to Information, Information Management, Information Technology, Security and Project Management communities across the Government of Canada.

The ATIP Online Request solution, initially a pilot led by Citizenship and Immigration Canada (CIC), with the participation of SSC and TBS, was recognized in the Excellence in the ATIP category. The ATIP Online

Request service is part of the Government of Canada's commitment to modernizing services to Canadians while increasing its open information environment.

The solution provides a faster, easier and more convenient way for Canadians to submit ATIP requests. It also reduces processing costs for institutions. In its initial pilot phase, the service allowed clients to submit requests and fees online to CIC, SSC and TBS. Given the successful implementation of the pilot, the service has now been expanded to include 33 other government institutions.

During the reporting period, SSC received 77% of its *Privacy Act* requests online, with 95 requests received via the ATIP Online Request service. Only 28 *Privacy Act* requests were received via the postal mail service.

Complaints and Audits

Complaints

SSC was subject to one use and disclosure complaint to the Office of the Privacy Commissioner under the *Privacy Act* concerning the Employees' Charitable Campaign. Corrective measures were taken to prevent the incident from reoccurring, and the individual was satisfied with the early resolution.

Audits

During the reporting period, no audits involving SSC were completed by the Office of the Privacy Commissioner of Canada pursuant to section 37 of the *Privacy Act*.

However, on December 10, 2015, the Privacy Commissioner of Canada tabled the 2014–2015 Annual Report on the *Privacy Act* urging federal departments and agencies to develop and implement more rigorous procedures and safeguards to protect Canadians' personal information and highlighting the results of an earlier audit of the government's management of portable storage devices. The audit examined 17 institutions in detail, including SSC.

SSC agreed with all of the Commissioner's recommendations and, as part of its formal follow-up process for all audit recommendations, the Department is closely monitoring the implementation of the following actions:

1. In collaboration with partner organizations, ensure that all active smart phones are captured, either by user or contact name, in a registry by January 2016;

2. Remind partner organizations of their responsibilities under the Operating Standard for the Provision of Telecommunications Devices, including the sanitization of smart phones prior to disposal;

3. Assess the risk to personal information resulting from the lack of controls on connection of unauthorized USB storage devices on servers, and implement appropriate controls to address identified gaps and weaknesses;

4. Ensure that baseline security controls are implemented on all smart phones in use at partner organizations by January 2016;

5. Amend the Provision of Telecommunication Devices and Acceptable Use of Cellular Devices Standards to instruct users to comply with their respective organizations' protocols for reporting security incidents and privacy breaches;

6. Ensure that SSC employees who have access to partner organizations' information holdings are aware of the policies governing the use of portable storage devices, and provide guidance to mitigate the privacy risks inherent to the use of the devices; and implement standardized procedures for responding to incidents involving the loss or theft of smart phones.

Parliamentary Affairs

During the period under review, one Order Paper Question or “Written Question” was placed on the Order Paper by Members of Parliament with respect to data, information, or privacy breaches in government departments, institutions and agencies for 2015. SSC provided its written response, which was tabled as a sessional paper. Upon request, these are available to the public via the Library of Parliament.

Breaches

SSC had no material privacy breaches to report during the period.

Privacy Impact Assessments

Summaries of completed PIAs are posted on SSC’s Internet site: Publications – Access to Information and Privacy.

In 2015–2016, one PIA was completed and forwarded to the Office of the Privacy Commissioner of Canada and TBS, which was for the Email Transformation Initiative (ETI), your.email@canada.ca, which is a Government of Canada priority to move SSC and 42 partner organizations to one consolidated, efficient, secure and modern email system. To this end, Bell Canada, in partnership with CGI Information Systems and Management Consultants Inc., was selected through a competitive process to deliver the Government of Canada’s new email solution.

In keeping with the guidance from the Office of the Privacy Commissioner and the Treasury Board Directive on Privacy Impact Assessment, privacy risks identified in the PIA have been aligned with the 10 universal privacy principles found in the Canadian Standards Association’s Model Code for the Protection of Personal Information. In addition, several privacy measures have been built into the design of the new email system, such as encryption, username and password credentials, no data matching and extensive controls limiting access to only those who need to know.

The PIA and the accompanying privacy risk and security action plans will be monitored and updated to ensure that the documents remain relevant and form part of the ETI overall risk-management framework for the initiative.

RACI Model

To facilitate the PIA process, a RACI model was adopted to identify roles and responsibilities during projects. RACI is an abbreviation for:

- Responsible – who is responsible to do the work or part of it
- Accountable – who has the final decision and ultimate ownership of the project
- Consulted – who must be consulted before a decision or action is taken
- Informed – who must be informed that a decision or action has been taken

A RACI chart describes the participation by various roles in completing tasks or deliverables for a project or business process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes. Two RACI charts were developed and are attached to the published Directive on Conducting Privacy Impact Assessments as annexes:

- RACI for Enterprise PIAs – this chart identifies roles and responsibilities for PIAs relating to enterprise-wide projects and initiatives. Such PIAs are reviewed at the Security Risk Management Board for recommendation for approval at the Senior Management Board, chaired by the President of SSC.
- RACI for Internal PIAs – this chart identifies roles and responsibilities for PIAs relating to SSC internal services projects and initiatives. These PIAs are presented at the Director General Planning Committee for recommendation for approval at the Corporate Management Board, chaired by the Senior Assistant Deputy Minister of the Strategy branch.

Ongoing PIA Files

SSC continues to work on initiated PIAs and Privacy Risk Checklists for projects such as:

1. Videoconferencing Enterprise Service
2. Workplace Communication Service Internet Protocol Telephony (including Voice over Internet Protocol)
3. Hosted Contact Centre Service
4. Guest Wi-Fi Service
5. Government of Canada Internal Centralized Authentication Service
6. Government of Canada Managed Security Services
7. Personal Security Digitization
8. Port Management
9. Electronic Procurement and Payment
10. Conflict of Interest System and E-Forms
11. Emergency Attendance Report System
12. Workplace Technology Devices – Printing Products Procurement Project
13. Data Centre Consolidation

SSC continues to monitor the mitigation strategies identified in all PIA Actions Plans, such as the ETI.

Next Steps for the Year Ahead

SSC's ATIP Division appreciates the opportunity to be engaged in the development of a relatively new institution. It will continue to be innovative in its administration of the *Privacy Act* and take part in internal services transformation initiatives. The ATIP Division is committed to further supporting SSC as it instils a culture of service excellence and moves toward an efficient and modern paperless environment.

At the end of the reporting period, the ATIP Division was mapping its information holdings against SSC's 2015–2016 Program Alignment Architecture. This initiative will define SSC's information holdings in order to provide clarity to its *Info Source* chapter and will also assist requesters by directing their requests to the appropriate institution.

The ATIP Division will continue to develop knowledge and accountabilities for the ATIP Liaison Network and provide ATIP training and awareness opportunities for executives, managers and employees across the Department. During the last reporting year, the ATIP Division has been working in conjunction with the SSC Academy and the Canada School of Public Service (CSPS) to implement mandatory ATIP fundamentals training to all SSC employees by directing staff to the CSPS ATIP Fundamentals I015 online course. All current employees must successfully complete the course within three months of the course launch date. New employees to SSC will have three months from their date of arrival to complete the course. This mandatory course has a planned launch timeframe of May 2016. Also, in support of the yearly exercise of updating the SSC *Info Source* chapter, ATIP will be offering *Info Source* training.

In addition, an SSC ATIP priority over the next two years will be to develop a logic model and implement performance measurements for the ATIP Management Framework and its 14 policy instruments, along with desired outcomes, indicators and targets.

Annex A – Partner Organizations

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

Annex B – Delegated Authority

AUG 0 6 2015

***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 and Chief Privacy Officer
4. Director, Access to Information and Privacy Protection Division

Original signed by

Ron Parker

Ottawa,

Annex C – 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: 2015-04-01 to 2016-03-31

Part 1: Requests Under the *Privacy Act*

	Number of Requests
Received during reporting period	123
Outstanding from previous reporting period	0
Total	123
Closed during reporting period	120
Carried over to next reporting period	3

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	4	0	0	0	0	0	4
Disclosed in part	0	6	13	3	0	0	0	22
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	70	5	1	0	0	0	0	76
Request abandoned	17	1	0	0	0	0	0	18
Neither confirmed nor denied	0	0	0	0	0	0	0	0
Total	87	16	14	3	0	0	0	120

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	22
19(1)(f)	0	22.1	0	27	3
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)	0	70(1)(d)	0
69(1)(b)	0	70(1)(a)	0	70(1)(e)	0
69.1	0	70(1)(b)	0	70(1)(f)	0
		70(1)(c)	0	70.1	0

2.4 Format of information released

Disposition	Paper	Electronic	Other formats
All disclosed	1	3	0
Disclosed in part	5	17	0
Total	6	20	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	127	127	4
Disclosed in part	6141	3227	22
All exempted	0	0	0
All excluded	0	0	0
Request abandoned	0	0	18
Neither confirmed nor denied	0	0	0
Total	6268	3354	44

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	4	127	0	0	0	0	0	0	0	0
Disclosed in part	10	270	9	1539	1	653	2	765	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
Request abandoned	18	0	0	0	0	0	0	0	0	0
Neither confirmed nor denied	0	0	0	0	0	0	0	0	0	0
Total	32	397	9	1539	1	653	2	765	0	0

2.5.3 Other complexities

Disposition	Consultation Required	Legal Advice Sought	Interwoven Information	Other	Total
All disclosed	0	0	1	0	1
Disclosed in part	1	0	0	0	1
All exempted	0	0	0	0	0
All excluded	0	0	0	0	0
Request abandoned	0	0	0	0	0
Neither confirmed nor denied	0	0	0	0	0
Total	1	0	1	0	2

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 Subsections 8(2) and 8(5)

Paragraph 8(2)(e)	Paragraph 8(2)(m)	Subsection 8(5)	Total
0	0	0	0

Part 4: Requests for Correction of Personal Information and Notations

Disposition for Correction Requests Received	Number
Notations attached	0
Requests for correction accepted	0
Total	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	14	0	1	0
All exempted	0	0	0	0
All excluded	0	0	0	0
No records exist	1	0	0	0
Request abandoned	0	0	0	0
Total	15	0	1	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	15	0	1	0
Total	15	0	1	0

Part 6: Consultations Received From Other Institutions and Organizations

6.1 Consultations received from other Government of Canada institutions and other organizations

Consultations	Other Government of Canada 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 of Canada 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	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
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 Ddays	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
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

7.1 Requests with Legal Services

Number of Days	Fewer 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
1 to 15	0	0	0	0	0	0	0	0	0	0
16 to 30	0	0	0	0	0	0	0	0	0	0
31 to 60	0	0	0	0	0	0	0	0	0	0
61 to 120	0	0	0	0	0	0	0	0	0	0
121 to 180	0	0	0	0	0	0	0	0	0	0
181 to 365	0	0	0	0	0	0	0	0	0	0
More than 365	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0

7.2 Requests with Privy Council Office

Number of Days	Fewer 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
1 to 15	0	0	0	0	0	0	0	0	0	0
16 to 30	0	0	0	0	0	0	0	0	0	0
31 to 60	0	0	0	0	0	0	0	0	0	0
61 to 120	0	0	0	0	0	0	0	0	0	0
121 to 180	0	0	0	0	0	0	0	0	0	0
181 to 365	0	0	0	0	0	0	0	0	0	0
More than 365	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0

Part 8: Complaints and Investigations Notices Received

Section 31	Section 33	Section 35	Court action	Total
1	0	0	0	1

Part 9: Privacy Impact Assessments (PIAs)

Number of PIA(s) completed	1

Part 10: Resources Related to the *Privacy Act*

10.1 Costs

Expenditures		Amount
Salaries		$367,443
Overtime		$73
Goods and Services		$44,183
• Professional services contracts	$0	
• Other	$44,183	
Total		$411,699

10.2 Human Resources

Resources	Person Years Dedicated to Privacy Activities
Full-time employees	4.17
Part-time and casual employees	0.24
Regional staff	0.00
Consultants and agency personnel	0.00
Students	0.50
Total	4.91

Note: Enter values to two decimal places.