



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

2014–2015



Table of Contents

Introduction 3
 Privacy Act..... 3
Institutional Mandate and Organization..... 4
 Mandate..... 4
 Organization 4
Delegated Authority 5
ATIP Division Structure 5
Dedicated to Access to Information and Privacy Excellence 6
Interpretation of the Statistical Report – Requests for Personal Information and Consultations 7
Institutional ATIP Training and Awareness Activities 10
ATIP Policy Instruments, Procedures and Initiatives..... 12
Complaints and Audits 17
Parliamentary Affairs..... 17
Breaches..... 18
Privacy Impact Assessments 18
Next Steps for the Year Ahead 19
Annex A – Partner Organizations..... 20
Annex B – Delegated Authority 21
Annex C – Statistical Report on the *Privacy Act* 22

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, 2014 to March 31, 2015.

Institutional Mandate and Organization

Mandate

Shared Services Canada (SSC) is a federal department created on August 4, 2011 to transform how the Government of Canada manages its information technology (IT) infrastructure. SSC's mandate was reinforced on June 29, 2012 with the passage by Parliament of the [Shared Services Canada Act](#).

SSC's focus is to transform how the Government of Canada manages its IT infrastructure, by delivering modern, reliable, secure, cost-effective IT infrastructure to 42 partner organizations. The aim is to maintain and improve IT services delivery across the Government of Canada, generate and reinvest savings, enhance security, and implement government-wide solutions to transform the IT infrastructure to improve services to Canadians.

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 the partner departments and agencies ("Partner Organizations", refer to Annex A) in a modernized, consolidated and standardized manner to support the delivery of Government of Canada programs and services. During 2014–2015, SSC worked toward consolidating a new enterprise email system for the Government of Canada. In addition, the Department continued to consolidate data centres and telecommunication networks, as well as streamline the procurement of IT hardware and software used in the workplace. SSC also continued to support the achievement of Canada's Cyber Security Strategy.

In addition, SSC contributes to the achievement of other critically important and transformational Government of Canada initiatives, such as the Perimeter Security Defence Project, the Transformation of Pay Administration initiative and the vision of the public service of the future as articulated in Blueprint 2020. As an IT security service delivery organization, SSC works collaboratively with other Government of Canada cyber security agencies to support the cyber security strategy.

Organization

During the reporting period, SSC had four branches, each responsible for supporting one of the four elements of SSC's business model:

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

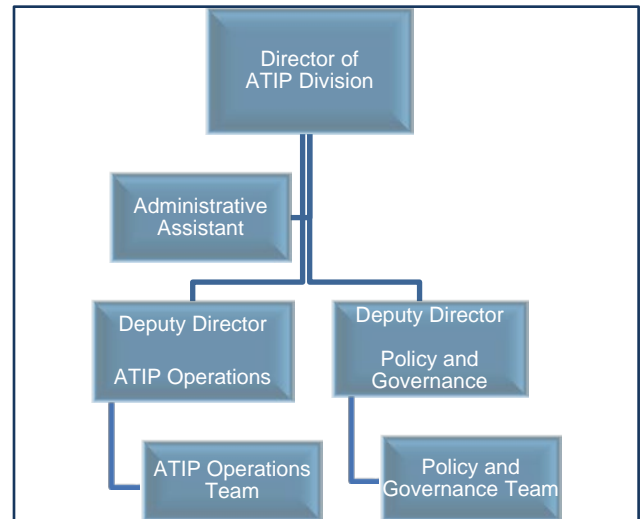
Although the branches were responsible for delivering on the priorities within each of their business lines, one of SSC's strengths is the synergies that occur when the various branches work together to deliver IT infrastructure services to SSC's Partner Organizations.

Delegated Authority

In April 2012, pursuant to section 73 of the [Privacy Act](#), the President of SSC delegated full powers, duties and functions under the [Act](#) to levels down to and including the Director of the Access to Information and Privacy Protection (ATIP) Division, hereafter referred to as the ATIP Division. (See Annex B)

ATIP Division Structure

During the period covered by this report, the ATIP Division structure had 16 full-time positions: the Director, two Deputy Directors, one Team Leader, 11 analysts and one administrative assistant. The ATIP Division maintained an average of 12.85 full-time equivalents, 4.76 of whom were dedicated to the administration of the [Privacy Act](#). By the end of the reporting period, the ATIP Division had 15 positions staffed.



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 between 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 draft personal information-sharing agreements, and conduct privacy impact assessments (PIA) to ensure that privacy legislation is respected. It also liaises with employees and prepares and delivers training and awareness sessions throughout SSC. In addition, the unit coordinates 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 anniversary month is June.

Dedicated to Access to Information and Privacy Excellence

The ATIP Division is responsible for developing, coordinating, 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, coordinating 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 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 coordinating the retrieval of records and recommendations from within their branch or region;
- Monitoring institutional compliance with both Acts and its 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 Information and Privacy 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; 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 2014–2015 reporting period.

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

During the reporting period, the ATIP Division received 71 requests under the [Privacy Act](#). There were no consultations under the [Privacy Act](#) from other government institutions. With one request carried forward from the previous reporting period, the ATIP Division processed a total of 72 requests.

The volume of requests received under the [Privacy Act](#) during this reporting period was comparable to the previous reporting period (in which 69 requests had been received). Out of 3,255 pages received and processed by the ATIP Division, 2,601 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, Part 1 and Part 2, Table 2.1)

During this reporting period, 71 requests were received under the [Privacy Act](#). One request from the previous reporting period was carried forward, for a total of 72 requests requiring action for this reporting period. Seventy-two requests were completed before the end of the reporting period.

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

Of the 72 requests completed, four led to the full disclosure of the requested documents, eight had exemptions applied to parts of the records prior to their release, and none had exemptions applied to the records in their entirety.

While it is being reported that no records existed for 55 requests, it should be noted that 52 of these requests related to records under the control of other government institutions and were redirected accordingly. These redirects were due to the [Access to Information and Privacy \(ATIP\) Online Request](#) web service, through which SSC had received requests intended for other institutions. No records existed for the remaining three requests.

For various reasons, five 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 72 requests, 68 (over 94%) were completed by the 30-day deadline established by the Act, with the remaining 3 requests 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, such as information related to law enforcement investigations, information about other individuals or information that is subject to solicitor-client privilege, be exempted and not released.

During the reporting period, there were eight 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 no other exemptions invoked in relation to the requests.

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.

Extensions (Annex C, Part 5, Table 5.1)

Extensions permissible under section 15 of the Act were claimed for three requests. In all cases, the extensions were sought for 30 additional days because of the requirement to review large volumes of information.

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 8)

According to the information provided by SSC's Finance Division in April 2015, during the reporting period, the ATIP Division spent \$325,495 on salaries and \$97,420 on goods and services, including professional service contracts, for the administration of the [Privacy Act](#).

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 on privacy. 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.

A total of ten ATIP sessions were delivered to approximately 180 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 Director of ATIP delivered six sessions to ATIP Liaison Officers and their delegates (65 participants). In addition, the Deputy Director of ATIP Operations addressed a Branch's specific training requirements by giving a tailored overview to administrative assistants and Liaison Officers concerning types of ATIP response sheets, context around tasking, Notice of Release processes and responded to related questions (15 participants).

ATIP Training for Subject Matter Experts in Offices of Primary Interest (OPI)

Since the number and complexity of requests submitted to SSC was increasing, several program areas requested training on the ATIP process and the nature of exemptions. A 2.5-hour 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 Director of ATIP delivered three tailored OPI training sessions, one for the Cyber and IT Security Branch, another for the Extended Enterprise Projects Execution Leadership Team and a third session for the entire staff of the Chief Information and Security Office. All training initiatives were very well received and deemed worthwhile (100 participants).

Privacy in the Human Resources Environment

In the previous reporting period, the Human Resources and Workplace Directorate was offered some targeted training for Human Resources staff given the nature of their work. This reporting period saw informal, individual training specific to the development of PIAs, and the completion of Privacy Risk Checklists. This informal, individual training will be ongoing.

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 (RTK) Week

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. In 2014, the Canadian RTK Week took place from September 22 to 28. SSC promoted RTK Week by highlighting the week in its weekly bulletin to employees and encouraging them to participate in events in their regions and to help protect information by following the Department's clean desk guidelines.

Data Privacy Day

On January 28, 2015, 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 joint communiqué to employees from the Chief Privacy Officer and Director, ATIP Division, highlighting that:

- in August 2014, TBS replaced its [Policy on Privacy Protection](#), and informing employees what is expected of them concerning the requirements of the [Privacy Act](#); and
- in November 2014, SSC launched the Department's [Access to Information and Privacy Management Framework](#), [Directive on Privacy Breaches](#) and [Standard on Managing Privacy Breaches](#).

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

ATIP Awareness for Managers Network

The ATIP Division collaborated with the SSC Managers Network and the Administrative Professionals Network to promote awareness. In November, a message was sent to all SSC managers informing them of SSC's Access to Information and Privacy Internal Policy Instruments and the important role they play in preventing privacy breaches.

ATIP Policy Instruments, Procedures and Initiatives

During this reporting period, SSC continued to work toward embedding a culture of privacy excellence. The Department finalized several policy instruments and updated the inventory of its personal information holdings in *Info Source* vis-à-vis its 2013–2014 Program Alignment Architecture.

ATIP Management Framework

During the reporting period, the ATIP Division introduced an [ATIP Management Framework](#), which sets out a comprehensive governance and accountability structure that, among other things, reflects SSC's responsibilities under both the [Access to Information Act](#) and the [Privacy Act](#) with respect to access rights and with regard to SSC's collection, use, disclosure, retention and disposal of personal information.

In 2014–2015, the Framework was approved, implemented, posted on SSC's extranet site and communicated to employees via a communiqué from SSC's President and Chief Operating Officer. It explains how SSC is organized in terms of its structures, policies, systems and procedures for, among other things, managing privacy risks, assigning privacy responsibilities, coordinating privacy work and ensuring compliance with the [Privacy Act](#), the [Access to Information Act](#), related TBS policies and directives, and internal ATIP-related policies.

To complement the ATIP Management Framework, the ATIP Division drafted a series of policy instruments to provide guidance to SSC employees. The following privacy policy instruments were approved, implemented and posted on SSC's extranet site in the reporting period:

1. [Directive on Privacy Breaches](#) – contains requirements, responsibilities and accountabilities that support SSC in meeting its obligations to manage privacy breaches.
2. [Standard on Managing Privacy Breaches](#) – supports privacy management at SSC by providing comprehensive governance and accountability in responding to privacy breaches.

The following ATIP policy instruments were still in development at the end of this reporting period:

1. *Directive on Access to Information and Privacy Training and Awareness* – supports SSC in embedding ATIP excellence through training and awareness.
2. *Directive on Conducting Privacy Impact Assessments* – supports SSC in meeting its obligations to manage privacy risks.
3. *Directive on Managing Personal Information Required for Administrative and Criminal Investigations* – supports SSC in managing the handling of personal information that is required for internal administrative investigations, and personal information that is required for external criminal investigations.
4. *Directive on Monitoring ATIP 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.

-
5. *Standard on the Code of Privacy Principles* – ensures that every reasonable measure is taken to reduce potential risks of privacy invasions, or privacy breaches concerning personal information entrusted to employees.
 6. *Standard on Managing Privacy in Emergencies* – establishes best practices for handling personal information in emergency situations, with recognition of the fact that emergencies will differ in their severity and context.
 7. *Standard on Preventing and Managing Obstruction to the Right of Access* – establishes the procedures for addressing instances of perceived and actual obstruction of lawful access to information under SSC's control.
 8. *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.
 9. *SSC Social Media Privacy Checklist* (a companion to # 8.) – determines if a PIA is required or whether a full PIA or an amendment to an existing PIA must be completed, and ascertains if there are any privacy risks with the proposed social media activity.

“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.
- 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's policies and guidelines. They provide important checks and balances required to maintain SSC's continued 100% compliance rate.

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 the 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 is an important part of SSC's processing of requests. Further, a process has been established to enable Partner Organizations to conduct searches of their data held on any SSC server where such searches are necessary in order to properly respond to a [Privacy Act](#) request. In such cases, the ATIP Division of the relevant Partner Organization is required to contact its institutional Chief Information Officer, who serves as the primary point of contact between the Partner Organization and SSC's account executives.

Info Source Modernization Initiative

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 and 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 the 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. TBS commented that, "*Shared Services Canada has worked diligently to ensure their chapter meets TBS requirements. This is an excellent decentralized published Info Source chapter. Well done!*"

ATIP Online Request Service

During the reporting period, SSC received 65 [Privacy Act](#) requests via the [Access to Information and Privacy \(ATIP\) Online Request](#) service. Six [Privacy Act](#) requests were received via paper mail service. While the majority of these requests were misdirected to SSC, it is expected that this number will continue to decline as more institutions are added to the ATIP online service.

ATIP Community Development Initiative

The SSC ATIP Division was also the lead working closely with the federal ATIP community to create generic organizational models and work descriptions for the federal public service. Throughout the process there have been many consultations with the ATIP community at large and other stakeholders, including the Public Service Alliance of Canada. The aim is to eventually have standardized recruitment and staffing tools for the ATIP community.

Complaints and Audits

Complaints

SSC was subject to one complaint under the [Privacy Act](#).

In November 2014, the ATIP office received a privacy complaint from an SSC employee concerning a targeted email received from a Government of Canada Workplace Charitable Campaign coordinator. The email encouraged a donation this year, mentioning the employee's contribution in the previous year. The SSC employee filed a complaint under the [Privacy Act](#) to the Office of the Privacy Commissioner of Canada concerning the improper use and disclosure of personal information.

The fact that an individual has or has not made a donation is a personal matter and should not be shared without the individual's consent. Upon being made aware of the complaint, the ATIP Division immediately contacted all Campaign Leaders and took action to contain the incident and minimize the risk of such recurrence in future campaigns.

Audits

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

Parliamentary Affairs

During the period under review, six Order Paper Questions or "Written Questions" regarding access to information and/or privacy were placed on the Order Paper by Members of Parliament. SSC provided written responses, which were tabled as sessional papers. 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 2014–2015, two PIAs were completed and forwarded to the Office of the Privacy Commissioner of Canada and TBS:

- [Employee Experience and Skills Inventory](#)
The Employee Experience and Skills Inventory is a data set on employee experience and skills. The collection and analysis of this data (acquired via the Employee Experience and Skills Questionnaire) will help SSC properly plan its resources, offer increased opportunities to employees, ensure sound management of its workforce, advance the corporate-wide learning and development approach, and develop its workforce.
- [Government Electronic Directory Services 2.0](#)
GEDS 2.0 is a new version of the Government Electronic Directory Services (GEDS) program. It has been completely redesigned, re-architected and rewritten to provide both public and internal access to data stored in the GEDS database. While the employee contact information available to the public remains the same, GEDS 2.0 introduces a database internal to public servants. The “MyGEDS” data includes a personal photo, an employee profile, additional contacts, website links and employee competencies and competency search tags. MyGEDS also allows employee postings on Government of Canada 2.0 tools (GCconnex, GCpedia and GCforums) to be displayed when viewing MyGEDS.

Also of note is that, in addition to other ongoing PIAs for both transformation initiatives and internal services program activities, extensive work was done by the ATIP Division throughout the fiscal year on the PIA for the Email Transformation Initiative (ETI). The ATIP Division worked closely with SSC's ETI Project Authority team and the IT Security and Privacy Risk Assessment Division in the review and assessment of the privacy implications for this new email solution. This working group's weekly meetings continued into the next fiscal year 2015–2016.

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.

The ATIP Division will map its information holdings against SSC's 2014–2015 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 has also drafted several other policy instruments and is working towards approval, implementation and communication during 2015–2016. The status will be reported in next year's Annual Report. These policy instruments include:

1. *Directive on Access to Information and Privacy (ATIP) Training and Awareness*
2. *Directive on Conducting Privacy Impact Assessments*
3. *Directive on Managing Personal Information Required for Administrative or Criminal Investigations*
4. *Directive on Monitoring ATIP Compliance*
5. *Standard on the Code of Privacy Principles*
6. *Standard on Managing Privacy in Emergencies*
7. *Standard on Preventing and Managing Obstruction to the Right of Access*
8. *Standard on the Use of Personal Information for Non-Administrative Purposes*

In addition, SSC will continue to work on initiated PIAs, such as for these projects:

1. Email Transformation Initiative
2. Conflict of Interest eForm
3. Electronic Procurement and Payment
4. Videoconferencing Enterprise Service

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.

Annex A – 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 Northern Economic Development Agency
11. Canadian Nuclear Safety Commission
12. Canadian Space Agency
13. Citizenship and Immigration Canada
14. Correctional Service Canada
15. Department of Finance Canada
16. Department of Justice Canada
17. Employment and Social Development Canada
18. Environment Canada
19. Federal Economic Development Agency for Southern Ontario (FedDev Ontario)
20. Financial Transactions and Reports Analysis Centre of Canada
21. Fisheries and Oceans Canada
22. Foreign Affairs, Trade and Development Canada
23. Health Canada
24. Immigration and Refugee Board of Canada
25. Industry Canada
26. Infrastructure 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 Works and Government Services 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



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 C – Statistical Report on the *Privacy Act*

Name of institution: Shared Services Canada

Reporting period: 2014-04-01 to 2015-03-31

Part 1: Requests Under the *Privacy Act*

	Number of Requests
Received during reporting period	71
Outstanding from previous reporting period	1
Total	72
Closed during reporting period	72
Carried over to next reporting period	0

Part 2: Requests Closed During the Reporting Period

2.1 Disposition and completion time

Disposition of Requests	Completion Time							Total
	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	
All disclosed	2	2	0	0	0	0	0	4
Disclosed in part	0	5	3	0	0	0	0	8
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	55	0	0	0	0	0	0	55
Request abandoned	3	1	1	0	0	0	0	5
Neither confirmed nor denied	0	0	0	0	0	0	0	0
Total	60	8	4	0	0	0	0	72

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	8
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)	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	3	1	0
Disclosed in part	4	4	0
Total	7	5	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	373	364	4
Disclosed in part	2228	1371	8
All exempted	0	0	0
All excluded	0	0	0
Request abandoned	0	0	5
Neither confirmed nor denied	0	0	0
Total	2601	1735	17

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	3	7	1	357	0	0	0	0	0	0
Disclosed in part	2	64	5	659	1	648	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
Request abandoned	5	0	0	0	0	0	0	0	0	0
Neither confirmed nor denied	0	0	0	0	0	0	0	0	0	0
Total	10	71	6	1016	1	648	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
Request abandoned	0	0	1	0	1
Neither confirmed nor denied	0	0		0	0
Total	0	0	1	0	1

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	3	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	3	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	3	0	0	0
Total	3	0	0	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							Total
	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	
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							Total
	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	
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
0	0	0	0	0

Part 9: Privacy Impact Assessments (PIAs)

Number of PIA(s) completed	2
----------------------------	---

Part 10: Resources Related to the *Privacy Act***10.1 Costs**

Expenditures		Amount
Salaries		\$325,495
Overtime		\$0
Goods and Services		\$97,420
• Professional services contracts	\$75,679	
• Other	\$21,741	
Total		\$422,915

10.2 Human Resources

Resources	Person Years Dedicated to Privacy Activities
Full-time employees	4.13
Part-time and casual employees	0.40
Regional staff	0.00
Consultants and agency personnel	0.11
Students	0.12
Total	4.76

Note: Enter values to two decimal places.

Annual Report to Parliament on the Administration of the Privacy Act – 2014-2015 (Shared Services Canada)

Issued also in French under title: Rapport annuel au Parlement sur l'administration de la Loi sur la protection des renseignements personnels – 2014-2015

ISSN 2369-4610

Key title: Annual Report to Parliament on the Administration of the Privacy Act – 2014-2015

Information contained in this publication or product may be reproduced, in part or in whole, and by any means, for personal or public non-commercial purposes, without charge or further permission, unless otherwise specified.

You are asked to:

- Exercise due diligence in ensuring the accuracy of the materials reproduced;
- Indicate both the complete title of the materials reproduced, as well as the author organization; and
- Indicate that the reproduction is a copy of an official work that is published by the Government of Canada and that the reproduction has not been produced in affiliation with or with the endorsement of the Government of Canada.

Commercial reproduction and distribution is prohibited except with written permission from Shared Services Canada (SSC). For more information, please contact Shared Services Canada at SSC.information-information.SPC@canada.ca.

© Her Majesty the Queen in Right of Canada, as represented by the Minister responsible for Shared Services Canada, 2015
Cat. No. P115-5E-PDF
ISSN 2369-4610