



2018-2019



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



Shared Services
Canada

Services partagés
Canada

Canada

Table of Contents

Introduction	3
<i>Privacy Act</i>	3
Institutional Mandate	4
Delegated Authority	4
ATIP Division Structure	4
Highlights of the 2018-2019 Statistical Report	6
Requests Received	6
<i>Disposition of Requests Completed</i>	7
<i>Extensions</i>	7
<i>Completion Time</i>	7
<i>Exemptions</i>	8
<i>Exclusions</i>	8
<i>Consultations</i>	8
Complaints, Audits and Investigations	9
Monitoring Compliance	9
Disclosure of Personal Information Pursuant to Paragraphs 8(2)(e) and 8(2)(m)	9
Training and Awareness Activities	10
Initiatives	11
Policies, Guidelines and Procedures	11
Material Privacy Breaches	12
Privacy Impact Assessments	12
Next Steps for the Year Ahead	14
Annex A – Designation Order	15
Annex B – Statistical Report	16
Annex C – New Exemptions under the <i>Privacy Act</i>	23

Introduction

Shared Services Canada (SSC) is pleased to submit to Parliament its 8th annual report on the administration of the [Privacy Act](#). The report describes how SSC administered the *Privacy Act* for the fiscal year commencing April 1, 2018 and ending March 31, 2019.

Privacy Act

The *Privacy Act* came into effect on July 1, 1983. The *Privacy 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.

Institutional Mandate

SSC was created in 2011, to transform how the government manages and secures its information technology (IT) infrastructure.

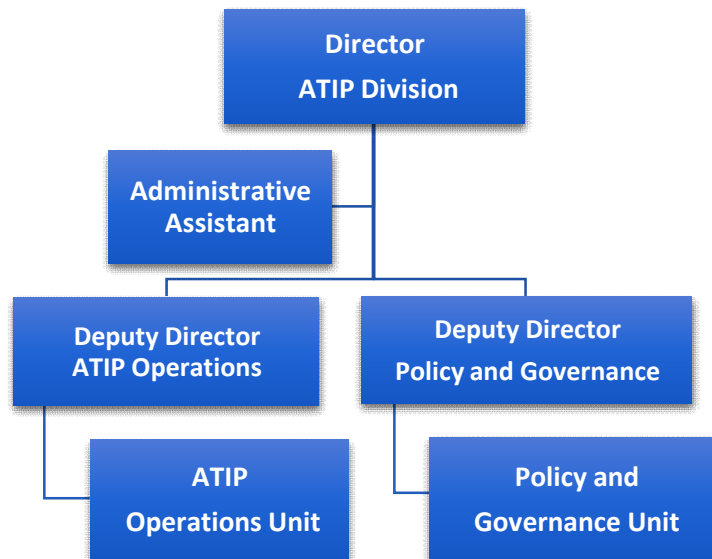
SSC plays a key role in the government's ability to deliver digital programs and services that improve the lives of Canadians, their families and communities.

SSC works in partnership with key public-sector and private-sector stakeholders to implement enterprise-wide approaches for managing IT infrastructure services and employ effective and efficient business management processes. Maintaining strong customer relationships and service management is essential to the successful delivery of SSC's mandate.

Delegated Authority

SSC's President is responsible for handling requests submitted under the *Privacy Act*. Pursuant to Section 73 of the Act, the President has delegated full powers, duties and functions to members of the Department's senior management, including the Director and Deputy Directors of the Access to Information and Privacy (ATIP) Protection Division, hereafter referred to as the ATIP Division (Refer to Annex A)

ATIP Division Structure



The ATIP Division is part of the Corporate Secretariat, which is overseen by the Director General, Corporate Secretariat and Chief Privacy Officer, situated in the Corporate Services Branch at SSC.

The Division is led by a Director who is also the ATIP Coordinator for the Department, and is supported by two Deputy Directors, each leading either Operations or Policy and Governance. While an average of 21 person years were dedicated to the ATIP program, just over six person years were dedicated to the administration of the *Privacy Act*. These person years include full-time employees and students.

The Operations Unit within the ATIP Division is responsible for processing requests under the *Privacy Act* and 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 team also provides briefings to senior management as required on matters relating to requests and institutional performance. This team is also the main point of contact with the Office of the Privacy Commissioner (OPC) and Office of the Information Commissioner (OIC) 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 team also develops ATIP policy instruments and tools. The Unit is responsible for assisting program officials when they conduct privacy impact assessments (PIAs) 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 team coordinates SSC's annual reporting requirements and publishes SSC's [Info Source chapter](#). Lastly, the Unit is the main point of contact with the OPC and OIC with respect to various audits, reviews, systemic investigations and privacy breaches.

The Division's administration of the Acts is facilitated at the branch and directorate level of SSC. There are nine Liaison Officers who coordinate the collection of requested records and information, and provide guidance to branch and directorate managers on the application of the Acts.

Highlights of the 2018-2019 Statistical Report

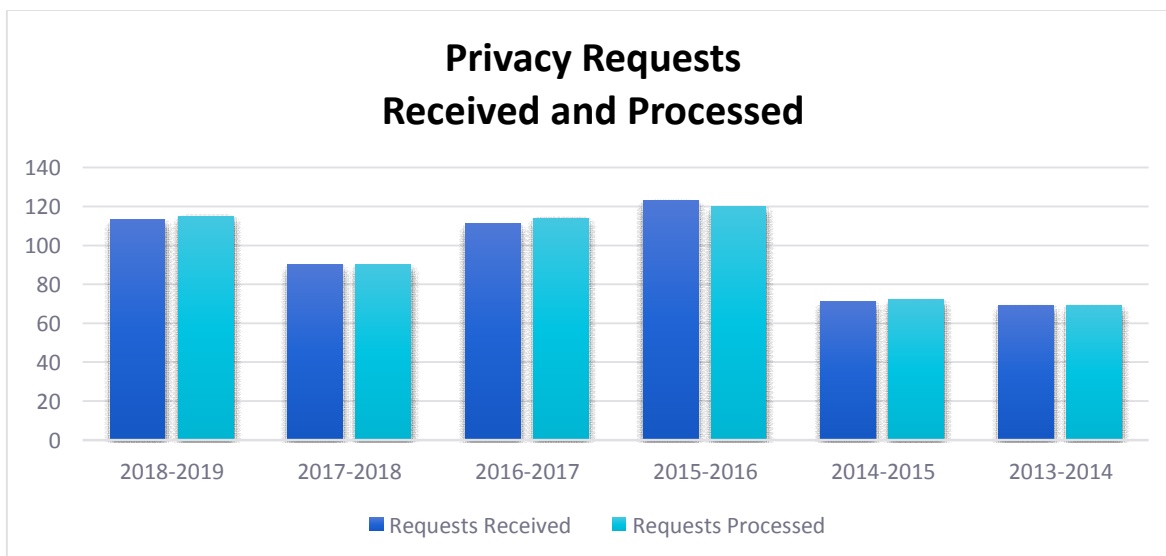
The Statistical Report (Annex B and C) on the administration of the *Privacy Act* provides a summary of the personal information requests and consultations processed during the 2018–2019 reporting period.

Requests Received

SSC received 113 requests submitted under the *Privacy Act* between April 1, 2018 and March 31, 2019. This total represents an increase of over 25 percent from the previous reporting period. Five requests were carried forward from 2017-2018 for a grand total of 118 requests for the reporting period. The number of requests received by the Department over the last five years has grown nearly 60 percent. Privacy requests received were mainly from SSC employees seeking their own personal file.

The Department processed 115 privacy requests representing an increase of over 35 percent from the previous fiscal year. In turn, the ATIP Division experienced a six fold rise in the number of pages processed at 65,413 pages for the 2018-2019 fiscal year. Similarly, the pages disclosed increased significantly from the previous fiscal year at 6,281 pages to 16,184 pages for the 2018-2019 reporting period. With the exception of one privacy request that was completed beyond the legislated timeframe, SSC maintained a 99 percent compliance rate.

The ATIP Division continues to ensure that it monitors its turnaround times in processing requests on a weekly basis as well as tracks the timeliness of their completion.



Disposition of Requests Completed

At the conclusion of the reporting period, 115 privacy requests were completed while five requests were carried over to the next fiscal year. Of these, SSC released records in full in four cases (3 percent), For 34 requests (30 percent), the Department invoked exemptions. Of the remaining 77 requests (67 percent), either no records existed or the request was abandoned.

Extensions

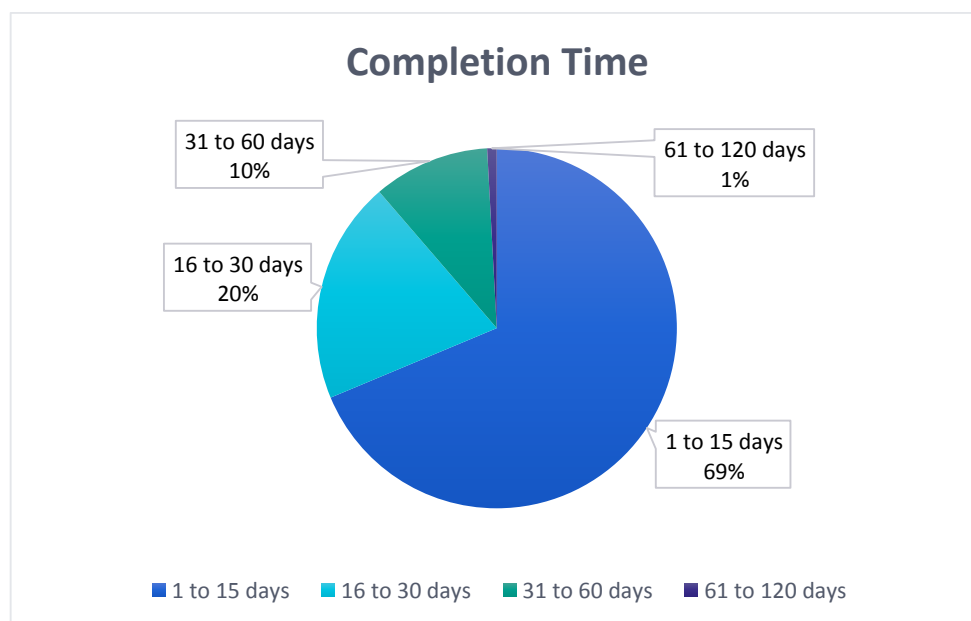
Section 15 of the *Privacy Act* allows the statutory time limits to be extended if consultations are required, if translation is needed or if the request is for a large volume of records, and processing it within the original time limit would unreasonably interfere with the operations of the Department.

SSC invoked a total of 13 extensions during the 2018-2019 reporting period, which were deemed necessary to search for or through a large volume of records and/or to respond to the higher volume of requests, which interfered with operations.

Completion Time

The *Privacy Act* sets the timelines for responding to privacy requests. It also allows for extensions in cases where responding to the request requires the review of a large volume of information or extensive consultations with other government institutions or other third parties.

SSC responded to 102 requests (89 percent) within 30 days or fewer, and a further 12 requests (10 percent) within 31 to 60 days. The Department completed one request (1 percent) within 61 to 120 days.



Exemptions

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, another individual besides the requester, or when it is subject to solicitor-client privilege.

The majority of exemptions applied by SSC related to Section 26 which protects personal information. The aforementioned section was applied in 33 instances. Section 22(1)(b) (law enforcement and criminal investigations) and Section 25 (safety of individuals) were each invoked once.

Exclusions

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. The ATIP Division did not apply any exclusions under the Act during the reporting period.

Consultations

During the reporting period, no consultation requests under the *Privacy Act* were received at SSC from other government departments.

Complaints, Audits and Investigations

SSC was not subject to any complaints under the *Privacy Act* during the reporting period. In addition, no audits or investigations involving the Department were conducted by the OPC.

Monitoring Compliance

The Division has implemented various internal procedures to ensure that privacy requests are processed in a timely and efficient manner. For example, meetings are held between ATIP management and analysts on a regular basis to monitor workloads and progress on privacy requests. These meetings provide greater accountability and clarity for the team.

In 2018-2019, SSC did not receive any requests to correct personal information under the *Privacy Act*.

Disclosure of Personal Information Pursuant to Paragraphs 8(2)(e) and 8(2)(m)

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. For the 2018-2019 fiscal year, SSC did not disclose any personal information under this paragraph.

Training and Awareness Activities

The ATIP Division is dedicated to fostering a culture of ATIP excellence across SSC. As a result, the Division continues to develop and deliver training and awareness activities aimed at more openness and transparency across the Department.

Mandatory Training

In order to ensure that all SSC employees, regardless of their position or level, are made aware of their responsibilities related to ATIP and that they gain an in-depth understanding of the related best practices and principles, SSC launched, in collaboration with the Canada School of Public Service (CSPS), the online Access to Information and Privacy Fundamentals course (I015) on July 14, 2016. While this course is optional for all federal public service employees through the CSPS website, its completion has been made mandatory for all SSC employees. For this reporting period, approximately 773 SSC employees successfully completed the course. This represents an 11 percent increase from last fiscal year.

The ATIP Division successfully delivered 25 internal training and awareness sessions to approximately 217 participants, which included SSC executives, managers and employees at all levels. The number of training provided this fiscal year increased by 79 percent. In the previous fiscal year, 14 training sessions were provided to SSC employees.

ATIP 101 Training

The Division delivered numerous ATIP 101 training sessions over the course of 2018-2019. A total of 103 employees completed this course.

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. During this reporting period, the ATIP Division delivered nine training sessions specifically tailored to our ATIP Liaison Officers and their delegates, to a total of approximately 83 participants. In comparison to the 2017-2018 fiscal period, two training sessions were delivered to 17 ATIP Liaison Officers.

ATIP Awareness for SSC Executives

During this reporting period, six awareness sessions were delivered to 31 executives. These sessions provide an overview of key ATIP principles and practices, and provide a greater understanding of the roles and responsibilities of managers and employees.

Data Privacy Day

On January 28, 2019, SSC observed Data Privacy Day to continue to raise awareness about the importance of privacy and the protection of personal information. Data Privacy Day is an internationally recognized event aimed at promoting privacy best practices. The ATIP Division hosted an information booth to provide privacy-related material and to answer queries from employees.

Initiatives

To maintain a high standard of excellence and to continuously improve client services under the Privacy Act, the Department undertook the following initiatives:

- SSC was onboarded to TBS' new ATIP Online Request System. This platform makes it easier and simpler for Canadians to submit ATIP requests through a centralized website.
- The ATIP Division met with departmental Liaison Officers on a bi-monthly basis in order to foster a better line of communication as well as to address emerging issues.
- The Operations Unit updated the actions, template emails and letters in the AccessPro Case Management system, the Division's case tracking and reporting software, to streamline the administration of ATIP requests.
- The Policy and Governance Unit developed a Training Strategy Plan for the delivery of training on the application of the *Access to Information Act* and *Privacy Act* to continue to educate all SSC employees on their roles and responsibilities related to ATIP. The new training plan placed heavy emphasis on privacy breaches, PIAs as well as training for the Offices of Primary Interest and Liaison Officers.
- ATIP took the preliminary steps to implement epost Connect, which allows for the electronic delivery of responsive records to requesters.
- The Division engaged key internal stakeholders and the ATIP community on the anticipated legislative and policy changes resulting from *Access to Information Act* and *Privacy Act* reform (Bill C-58). A working group was created consisting of key internal partners to modify and update SSC processes to ensure a speedy implementation upon the legislation receiving Royal Assent.

Policies, Guidelines and Procedures

- The ATIP Division provides monthly and quarterly reports to SSC branches aimed at helping to increase response times for responsive records.
- A new Privacy Breach Incident Report template was developed to ensure SSC employees are aware of the necessary steps to follow and report suspected cases of privacy breaches.
- The Division updated the *Directive on Conducting Privacy Impact Assessments* to better align it with the revised *Policy on Privacy Protection* and to properly reflect the roles and responsibilities of key stakeholders and account for changes within the Department. The Directive is awaiting senior management approval.
- ATIP worked collaboratively with the Information Management Division to adjust processes and increase training on permission control for GCDOCS, SSC's electronic records system. This ensured that personal information was properly safeguarded in an effort to reduce privacy breaches across the Department.

Material Privacy Breaches

During the reporting period, no material privacy breaches occurred or were reported to the OPC.

Privacy Impact Assessments

In keeping with the guidance from the OPC and TBS' [Directive on Privacy Impact Assessment](#), privacy risks identified in PIAs are aligned with the [ten universal privacy principles](#) found in the Canadian Standards Association's *Model Code for the Protection of Personal Information*. In addition, privacy and security controls are required to be in place during the life cycle of projects at SSC, as recommended through SSC's Functional Direction 6.0.

During the 2018-2019 fiscal year, SSC completed three PIAs. The Conflict of Interest and Declaration System and the Hosted Contact Centre Service PIA summaries are available on the Department's website: [Publications-Access to Information and Privacy](#). The third PIA summary, related to the Enterprise Mobile Device Management, is being prepared for online publication.

Conflict of Interest and Declaration System

The PIA summary can be found at the following link: <https://www.canada.ca/en/shared-services/corporate/transparency/access-information-privacy/publications/privacy-impact-assessment-coids.html>

The Conflict of Interest Declaration System (COIDS) replaces the COID eForm, previously paper-based, with an electronic system so that SSC employees can disclose assets, liabilities, outside employment, personal relationships and networks, post-employment and other activities that may potentially give rise to a real, apparent or potential conflicts of interest in relation to the official duties and responsibilities of their position.

In accordance with the [Values and Ethics Code for the Public Sector](#), the [Policy on Conflict of Interest and Post-Employment](#), [Shared Services Canada's \(SSC's\) Directive on Conflict of Interest and Post-Employment](#), and SSC's Organizational Code, all federal employees are required to complete a paper-based Confidential Report when they join the public service and also when their situation changes that could put them in a real, apparent or potential conflict of interest situation.

To enhance the protection of personal information, a design decision was made to include the date of birth in the verification process as a way to reduce the possibility of a security or privacy breach. With respect to the Personal Information Bank at issue, TBS confirmed that no changes were required to the Standard Personal Information Bank PSE 915 "Values and Ethics Codes for the Public Sector and Organizational code(s) of Conduct", because PSE 915 includes a reference to "biographical information".

Concerning the safeguarding of personal information, the Security Assessment and Authorization (SA&A) of the COIDS identified some residual risks were mitigated and accepted.

A Vulnerability Assessment was completed to address some of the risks. Currently, vulnerability scans are being conducted monthly to monitor the system.

Hosted Contact Centre Service

The PIA summary can be found at the following link: <https://www.canada.ca/en/shared-services/corporate/transparency/access-information-privacy/publications/privacy-impact-assessment-hosted-contact-centreservice.html>

The Hosted Contact Centre Service (HCCS) project oversees the procurement of, and migration to, a government-wide hosted, managed and tailored contact centre service. It allows SSC's partner departments and agencies to interact with Government of Canada clients efficiently and effectively.

The overall risk assessment rating for the PIA is medium, and an action plan was drafted for mitigation purposes.

SSC's HCCS provides an infrastructure to handle and protect information designated up to and including Protected B level. The HCCS went through a full Security Authorization and Authorization process. The PIA examined all residual risks in the resulting report.

Enterprise Mobile Device Management

When Blackberry decided to no longer produce Blackberry devices, SSC launched the Enterprise Mobile Device Management (EMDM) service for SSC and partner organization employees. The Department designed and delivered this service to:

1. introduce two new Mobile Device Platforms (iOS and Android); and
2. build a service strong enough to manage all Government of Canada mobile devices.

The authority to collect personal information for this service lies in Section 6 of the *Shared Services Canada Act* and Order-in-Council (PC) Numbers 2015-1071 and 2016-0368.

EMDM collects name and business contact information. This includes username and password for email services. It may also include the Government of Canada PKI credentials (PIB SSC PCU 606 - Internal Credential Management Services).

In reviewing the EMDM service, while SSC collects very little personal information:

- partner organizations are responsible for personal information under their control;
- the mobile device collects personal information such as biometric and password data it stores in its own internal secure enclave; and
- EMDM users may provide personal information knowingly or unknowingly directly to third parties. Example include IT Vendors such as Apple, Google, or by applications or "apps", which are not subject to the *Privacy Act*, program legislation or government privacy policies.

The PIA evaluated the new Samsung/Android and iOS Mobile Device Platforms as well as the new service infrastructure identified in the EMDM Roadmap 1.4 release.

The PIA did find privacy risks which were addressed through a team approach and the risk has since been lowered by employing the best technical solutions, security controls and user guidance.

Next Steps for the Year Ahead

The ATIP Division is committed to remaining innovative in its administration of the *Privacy Act*. Additionally, the Division will continue to be actively engaged in the Department's internal services transformation initiatives as well as continue to participate in federal ATIP Community meetings. ATIP will continue to support the departmental priority of fostering a culture of service excellence.

The Division has made significant inroads in moving completely to a paperless environment with the adoption and implementation of epost Connect. In pursuing such digital initiatives, ATIP is one step closer to its goal of eliminating the use of paper, and will continue to pursue other opportunities in the future to achieve the end result of a paperless office.

Annex A – 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.

This designation order supersedes any previous delegation of the powers, duties and functions set out herein.

Dated at Ottawa,
this 8th day of May 2019

Schedule

1. Executive Vice President
2. Senior Assistant Deputy Minister, Corporate Services
3. Corporate Secretary and Chief Privacy Officer
4. Director, Access to Information and Privacy Protection Division
5. Deputy Directors, Operations and Policy and Governance, Access to Information and Privacy Protection Division

Paul Glover
President of Shared Services Canada

Annex B – Statistical Report



Government of Canada
Gouvernement du Canada

Statistical Report on the *Privacy Act*

Name of institution: Shared Services Canada

Reporting period: 2018-04-01 to 2019-03-31

Part 1: Requests under the *Privacy Act*

	Number of requests
Received during reporting period	113
Outstanding from previous reporting period	5
Total	118
Closed during reporting period	115
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							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	3	19	11	1	0	0	0	34
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	63	1	1	0	0	0	0	65
Request abandoned	11	1	0	0	0	0	0	12
Neither confirmed nor denied	0	0	0	0	0	0	0	0
Total	79	23	12	1	0	0	0	115

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)	1	24(b)	0
19(1)(d)	0	22(1)(c)	0	25	1
19(1)(e)	0	22(2)	0	26	33
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	0	4	0
Disclosed in part	4	30	0
Total	4	34	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	707	436	4
Disclosed in part	64,706	15,748	34
All exempted	0	0	0
All excluded	0	0	0
Request abandoned	0	0	12
Neither confirmed nor denied	0	0	0
Total	65,413	16,184	50

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	122	0	0	1	314	0	0	0	0
Disclosed in part	3	119	11	1,695	6	1,522	10	4,219	4	8,193
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	12	0	0	0	0	0	0	0	0	0
Neither confirmed nor denied	0	0	0	0	0	0	0	0	0	0
Total	18	241	11	1,695	7	1,836	10	4,219	4	8,193

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	16	0	16
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	0
Total	0	0	17	0	17

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
1	1	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	1	0	1
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	1	0	1

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	13	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	13	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	13	0	0	0
Total	13	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 for 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 PIAs completed	3
--------------------------	---

Part 10: Resources related to the *Privacy Act*

10.1 Costs

Expenditure	Amount
Salaries	\$529,150
Overtime	\$0
Goods and services	\$0
• Professional services contracts	
• Other	
Total	\$529,150

10.2 Human Resources

Resources	Person years dedicated to privacy activities
Full-time employees	5.50
Part-time and casual employees	0.00
Regional staff	0.00
Consultants and agency personnel	0.00
Students	1.00
Total	6.50

Annex C – New Exemptions under the *Privacy Act*

SSC is pleased to report on the two new exemptions (Sections 22.4 and 27.1) under the *Privacy Act*. In respect to the sections outlined below, the Department has not applied these exemptions during the 2018-2019 fiscal year.

<i>Privacy Act</i>	
Section	Number of requests
22.4 National Security and Intelligence Committee	0
27.1 Patent or Trademark privilege	0