2020 2021

ANNUAL REPORT TO PARLIAMENT

on the Administration of the *Privacy Act*

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

Introduction

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.

Shared Services Canada (SSC) is pleased to submit to Parliament its tenth Annual Report on the Administration of the *Privacy Act*. This report is prepared and tabled in Parliament in accordance with section 72 of the *Privacy Act*. It covers the period from April 1, 2020, to March 31, 2021.

Institutional Mandate

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

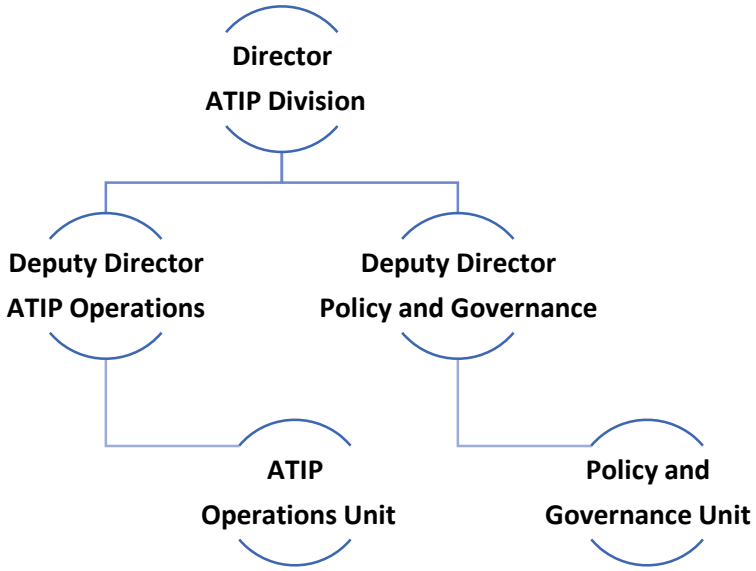
SSC supports the Government of Canada's digital vision to expand and improve the scope of digital service capacity, accelerate the pace of digital modernization, and strengthen the ongoing support for digital tools, systems and networks government wide.

In carrying out its mandate, SSC is supporting the Digital Operations Strategic Plan: 2018-2022 and the *Government of Canada Cloud Adoption Strategy*, as well as working in partnership with public- and private-sector stakeholders, implementing enterprise-wide approaches for managing IT infrastructure services, and employing effective and efficient business management processes.

Delegated Authority

The Minister of Digital Government is responsible for handling requests submitted under the *Privacy Act*. Pursuant to section 73(1) of the Act, the Minister has delegated full powers, duties and functions to members of the Department's senior management, including the Director and the 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 Secretary and Chief Privacy Officer, situated within the Strategy and Engagement Branch (SEB).

The division administers the *Access to Information Act* and the *Privacy Act,* led by a Director who acts as the ATIP Coordinator for the Department. Two units carry out the work under 2 Deputy Directors, each leading either the Operations Unit or the Policy and Governance Unit. While an average of 18 person-years were dedicated to the ATIP program, 6 person-years were dedicated to the administration of the *Privacy Act*. These person-years include full-time equivalents and students. Multiple staffing processes were completed during the year, including a joint Programme Administration (PM)-05 (Team Leader) process with the Treasury Board of Canada Secretariat (TBS).

The Operations Unit is responsible for processing requests under the *Access to Information Act* and the *Privacy Act*. This includes, but is not limited to the following:

- Liaising with subject-matter experts within SSC.
- Performing line-by-line reviews 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.
- Providing briefings to senior management as required on matters relating to requests and institutional performance.
- Acting as the main point of contact with the Office of the Information Commissioner (OIC) and the Office of the Privacy Commissioner (OPC) with respect to the resolution of complaints related to requests under both Acts.

The Policy and Governance Unit is responsible for, but is not limited to, the following:

- Providing policy advice and guidance to SSC's senior management team on access to information and the protection of personal information.
- Developing ATIP policy instruments and tools.
- Assisting program officials in conducting privacy impact assessments (PIA) and drafting personal information-sharing agreements.
- Preparing and delivering training and awareness sessions throughout SSC.
- Coordinating SSC's annual reporting requirements.
- Publishing an updated version of SSC's Info Source chapter.
- Acting as the main point of contact with the OIC and the OPC with respect to various audits, reviews, systemic investigations and privacy breaches.

The ATIP division's administration of the Acts is facilitated at the branch and the directorate level of SSC. There are 14 liaison officers at the Assistant-Deputy-Minister-Office level and 64 liaison officers at the branch level that coordinate the collection of requested records and information. In addition, they provide guidance to branch and directorate managers on the application of the Acts.

SSC was not party to any service agreements under section 73.1 of the *Privacy Act* and the *Access to Information Act* during the reporting period.

Highlights of the 2020–2021 Statistical Report

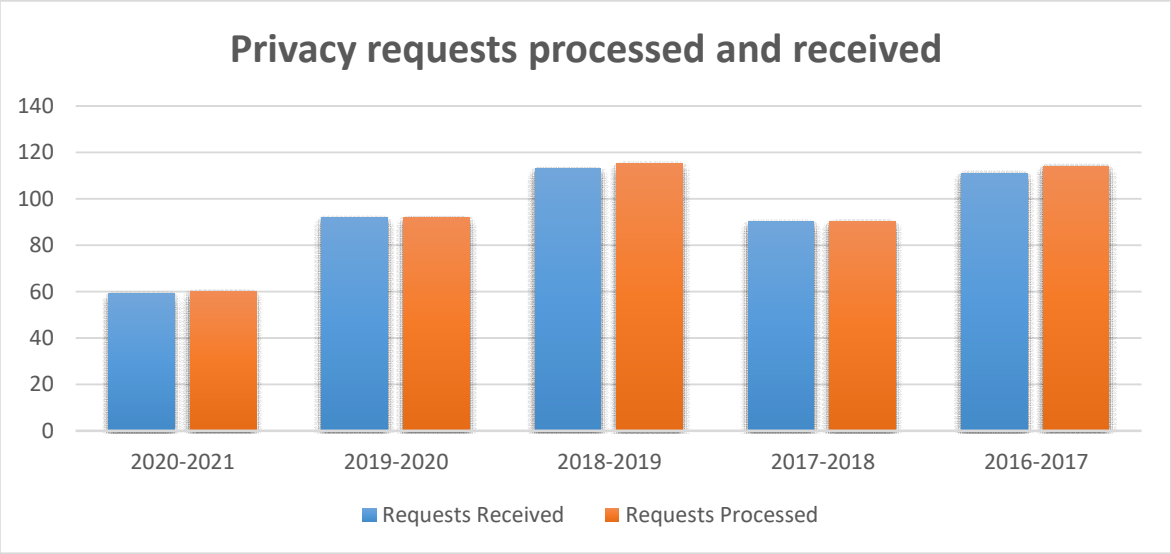
The Statistical Report (Annex B) on the administration of the *Privacy Act* provides a summary of the personal information requests and consultations processed during the 2020–2021 reporting period.

Requests Received

SSC received 59 requests submitted under the *Privacy Act* between April 1, 2020, and March 31, 2021. This total represents a decrease of 36 percent from the previous reporting period. Three requests were carried forward from 2019–2020 for a total of 62 requests for the reporting period. Privacy requests received were mainly from SSC employees seeking their own personal file.

SSC processed 60 privacy requests, and carried over 2 requests to the next fiscal year. The ATIP division experienced an increase in the number of pages processed at 38,385 pages for the 2020–2021 fiscal year. However, there was a 12-percent decrease in pages disclosed from the 2019–2020 reporting period.

It is important to note that SSC achieved a compliance rate of 98.3 percent. Although a slight decrease from last year's 100-percent mark, SSC is well above the community average. The ATIP division continues to ensure it monitors its turnaround times in processing requests on a regular basis, as well as tracks the timeliness of their completion.



Disposition of Requests Completed

At the conclusion of the reporting period, 60 privacy requests were completed while 2 requests were carried over to the next fiscal year. Of these, SSC released records in full in 1 case (2 percent) and the Department invoked exemptions in 21 requests (35 percent). Of the remaining 38 requests (63 percent), either no records existed, or the request was abandoned.

Extensions

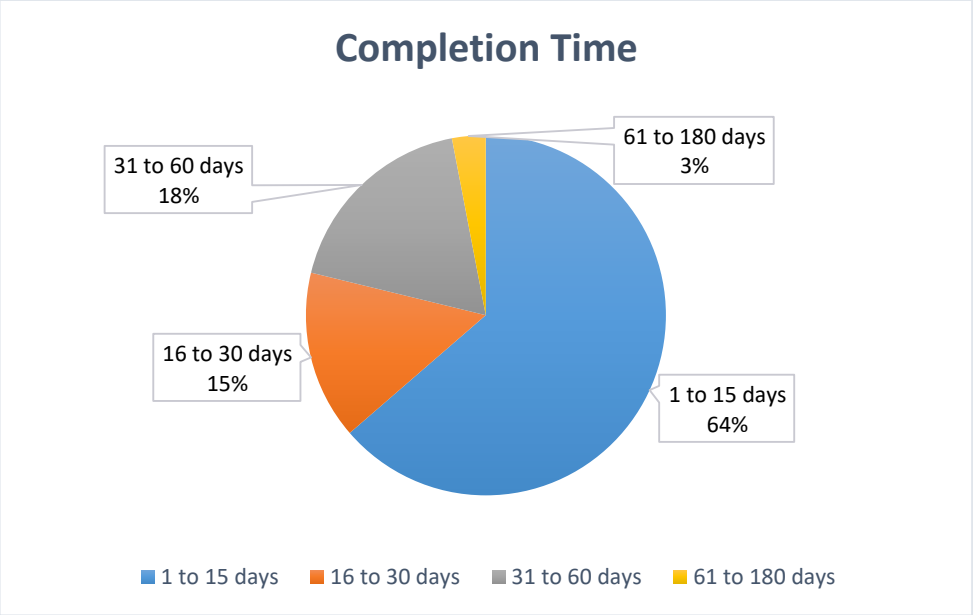
Section 15 of the *Privacy Act* allows the statutory time limits to be extended under certain circumstances, such as whether consultations are required, if translation is needed, or if the request is for a large volume of records, and processing it within the original time limit would unreasonably interfere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

SSC invoked a total of 13 extensions during the 2020–2021 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 47 requests (79 percent) within 30 days or fewer, and a further 11 requests (18 percent) within 31 to 60 days. The Department completed 2 requests (3 percent) within 61 to 180 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 19 instances. Section 22(1)(b) (law enforcement and criminal investigations) was used in 6 instances.

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.

Impact of COVID-19

The ATIP division was able to adapt quickly to the realities of working from home on a full-time basis. The majority of ATIP employees were already set up to work from home in the event of a building closure. Some of our accomplishments during the pandemic included the following:

- Operational from day one of the pandemic with the exception of the processing of Secret and Top Secret records. The office encountered no late files due to this restraint.
- Adapted all processes in order to continue to respond to requests from the Canadian public.
- Found solutions for consultations with other government departments and third parties. Paper and DVD format consultations were replaced by ePost and encrypted emails.
- Provided guidance to other institutions on the implementation of ePost.
- Provided hours of privacy advice to SSC senior leaders in relation to COVID-19.
- Participated in various collaborative working groups in order to address the current COVID-19 realities.
- Provided various advice and recommendations on Microsoft (MS) 365 suite, such as privacy notice statements and best practices for MS Teams and MS Stream.

The ATIP division was able to achieve these accomplishments while facing many challenges. Listed below are some of the major challenges faced by the division and what was done to overcome them:

- The lack of adequate office equipment at employees' homes affected their efficiency. Employees were able to enter the building individually and retrieve office equipment and supplies as directed by management. What could not be retrieved was purchased to accommodate employees.
- The ATIP division continued regular visits to the office in order to retrieve mail. No late files resulted due to early building closures.
- All requestors were advised that mailing of responsive records would be delayed as this could only be done once the ATIP division returns to the office. In order to prevent delays, ePost was used for all requests.
- Secret and Top Secret records must flow through the secure network that is only accessible at certain areas within SSC's office. Therefore, processing records above Protected B is still problematic. SSC is working on upgrading its infrastructure to more easily manipulate records with a Secret security classification.

- Mental health of employees was a concern. The Department provided COVID-19 support sessions to help employees with this challenge. In addition, management and coworkers supported each other during this period. The division shifted its priorities to focus primarily on essential tasks and introduced more flexible work schedules.

Complaints, Audits and Investigations

SSC was not subject to any complaints under the *Privacy Act* during the reporting period. In addition, there were no audits involving the Department conducted by the OPC. SSC received one notice of investigation from the OPC pursuant to section 31 of the *Privacy Act*.

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 2020–2021, 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 of the institution, 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 2020–2021 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 throughout 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, 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 Canada School of Public Service website, its completion has been made mandatory for all SSC employees. For this reporting period, 945 SSC employees successfully completed the course. This represents a 5-percent decrease from last fiscal year.

ATIP Internal Training

In order to maintain our training and awareness practices, the ATIP division was required to adapt their training from in-person to online. As a result, the trainers successfully delivered 31 internal training and awareness sessions to approximately 840 participants, which included SSC executives, managers and employees at all levels. The number of participants who received training this fiscal year increased by 71 percent. In the previous fiscal year, 490 SSC employees participated in training.

The division delivered numerous Privacy Breach training sessions over the 2020–2021 fiscal year. A total of 129 employees attended this course.

Data Privacy Day

On January 28, 2021, SSC celebrated Data Privacy Day to raise awareness, and demonstrate the importance of privacy and the protection of personal information in day-to-day activities. SSC's ATIP division delivered two Ask Me Anything virtual sessions to 160 employees, developed a pledge and communiqués, created graphics and recorded two "My Day in a Minute" videos of senior policy analysts. In addition, the Minister of Digital Government shared a video promoting the event. Awareness was disseminated through Twitter, LinkedIn and SSC's internal communication channels.

Policies, Guidelines, Procedures and Initiatives

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

- The Policy and Governance Unit developed a new Tasking Request training on the retrieval of records from offices of primary interest following an access to information request. The division continues to educate all SSC employees on their roles and responsibilities related to ATIP.
- The Policy and Governance Unit provided responses to over 150 requests for privacy advice to branches. These included privacy advice on newly onboarded MS365 tools, various privacy notice statements and the general strengthening of our privacy posture.
- The Policy and Governance Unit worked collaboratively with the Information Management division to increase awareness and training on permission control for GCdocs. This ensured that personal information continues to be properly safeguarded.
- To help program areas acquire a better understanding of privacy requirements and risks, the Policy and Governance Unit developed a new template for PIAs.
- The division assisted other government departments with their ePost onboarding, which allows for the electronic delivery of responsive records to requesters. With the addition of e-signatures for signing correspondence with requesters, SSC's ATIP division has been fully digital since the beginning of 2020.
- To further the knowledge of employees of the ATIP division, the following training was provided:
  - Plain language.
  - PIAs.
  - Investigating privacy breaches.
  - Negotiation skills training.
  - Internal biweekly learning sessions delivered by the SSC ATIP Director.

Material Privacy Breaches

A privacy breach refers to the improper or unauthorized access, collection, use, disclosure, retention or disposal of personal information. A material breach involves sensitive personal information that could reasonably be expected to cause serious injury or harm to the individual.

During the reporting period, one material privacy breach occurred and was reported to the OPC. The breach involved an employee accessing unauthorized files.

In this case, notification letters were sent to the affected individuals. The ATIP division provided recommendations and advice on mitigation measures to departmental staff in order to safeguard personal information. Both the OPC and TBS were notified of the breach. In addition, SSC senior officials, including the Chief Privacy Officer, were notified of the breach during various stages of the investigation.

The ATIP division monitors and documents all privacy breaches reported. The division also reviews how and where in the Department they occurred in order to provide tailored privacy breach training to specific groups to promote awareness and increase prevention.

Privacy Impact Assessments

One PIA was completed and signed at the President-level during the reporting period. Four PIAs were at various stages of the approval process at the end of the 2020–2021 fiscal year, they will be reflected on next year's report. The Policy and Governance Unit also completed 43 Privacy Risk Checklists. This checklist allows the team to determine if a PIA is required. It assesses new programs and initiatives used at SSC, as well as SSC's partners, in the collection, use, disclosure, storage and retention period of personal information. With the ATIP division's growing presence and awareness at SSC, program areas are reaching out more than ever for guidance and input. This is owing to the privacy-by-design vision at the beginning of new SSC initiatives, which explains the 169-percent increase for Privacy Risk Checklists.

Summaries of Completed Privacy Impact Assessments

Enterprise Perimeter Security

The Government of Canada has an obligation to protect all government assets including, but not limited to hardware, software, data and information assets. Today's biggest cybersecurity challenge is to provide robust safeguards to our Internet access points since they pose the largest attack vector and this problem is further exacerbated by the vast amount of encrypted traffic found along the Internet perimeter. In response to these issues, SSC has launched the Enterprise Perimeter Security (EPS) service to increase the visibility of cyber threats targeting Government of Canada networks to reduce the potential for compromising information and infrastructure assets of SSC and its partner departments and agencies. It also provides increased proactive monitoring, detection and response capabilities, thereby decreasing the risks to the confidentiality, integrity and availability of government assets. Ultimately, the EPS service can significantly strengthen the current Enterprise Government of Canada Internet Service by introducing several advanced capabilities, which includes the protection of network connections between ground and cloud boundaries.

The EPS intends to provide Government of Canada departments and agencies with a pre-assessed and authorized baseline system upon which each organization can build to meet their security requirements for Web browsing inspection needs. In addition, it intends to provide departments with the ability to safeguard their environments from malware while maintaining the availability, confidentiality and integrity of the information up to the Protected B level.

Although signed after March 31, 2021, SSC would like to highlight the Digital Communications and Collaboration (DCC) Initiative PIA (Microsoft 365 [M365])**.** The ATIP division drafted and implemented a communication strategy to consistently brief institutions that requested information regarding the PIA status. In addition, a sharing protocol that included a deliverable package was created to distribute the signed PIA quickly. This ensured consistent messaging was echoed in the ATIP community. The Digital Communications and Collaboration Initiative PIA (M365) has been shared with over 40 ATIP community partners.

Digital Communications and Collaboration Initiative PIA (M365)

SSC, on behalf of the Government of Canada, has acquired M365 E3 subscription licences for all Government of Canada employees. M365 is a combination of Office 365 E3, Enterprise and Mobility Services E3 and Windows 10 licences, plus Advanced Threat Protection licenced capability. Both Office 365 and Enterprise and Mobility Services are cloud-based software-as-a-service subscriptions.

The DCC Project is an SSC-led project that will validate the strategy, approach and network robustness for the rest of the Government of Canada's migration to a consistent, modern and comprehensive DCC service toolset. The purpose of starting with the DCC Project's pathfinders is to adopt an incremental implementation approach that leverages experience gained from these early adopters to inform the migration strategy, change management, network upgrades, identity and credential management, security monitoring and the Playbook components. This in turn will lead to more efficient processes for SSC, departments and agencies, identified in stream 2 (SSC partners) and other remaining departments in stream 3. SSC and Microsoft Consulting Services Inc. are working closely with the pathfinders and partners to ensure the pre-requisite remediation activities (e.g., network, active directory, change management) are completed on time.

SSC will provide the M365 platform to partners with guidance on the standard baseline configurations of their tenant spaces. Microsoft defines the services offered in the M365 space (e.g., Teams, One Drive, SharePoint, Exchange Online) as "workloads." SSC will deliver the network connectivity to the Microsoft cloud to connect departmental environments to M365 so they can begin to take advantage of the various "workloads." SSC will provide identity synchronization between on premise Active Directory and the Microsoft Azure Active Directory service and manage the infrastructure components that remain on premise that enable connectivity and data synchronization. Microsoft is responsible for the infrastructure components that support their cloud services.

Annex A—Delegation Order

Shared Services Canada

Access to Information Act and Privacy Act Delegation Order

The Minister of Digital Government, pursuant to subsection 95(1) of the *Access to Information Act* and subsection 73(1) of the *Privacy Act*, hereby designates the persons holding the positions set out in the schedule hereto, or the persons occupying on an acting basis those positions, to exercise the powers, duties and functions of the Minister as the head of Shared Services Canada, under the provisions of the acts and related regulations set out in the schedule opposite each position. This designation replaces all previous delegation orders.

Schedule

Position	*Access to Information Act* and Regulations	*Privacy Act* and Regulations
President	Full authority	Full authority
Executive Vice President	Full authority	Full authority
Corporate Secretary and Chief Privacy Officer	Full authority	Full authority
Director, Access to Information and Privacy Protection Division	Full authority	Full authority
Deputy Directors, Operations and Policy & Governance, Access to Information and Privacy Protection Division	Full authority	Full authority

Dated, at Ottawa this 26 day of June, 2020.

Services partagés Canada

Arrêté de délégation en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels

En vertu du paragraphe 95(1) de la *Loi sur l'accès à l'information* et du paragraphe 73(1) de la *Loi sur la protection des renseignements personnels*, la Ministre du Gouvernement numérique délègue aux titulaires des postes mentionnés à l'annexe ci-après, ainsi qu'aux personnes occupant à titre intérimaire lesdits postes, les attributions dont elle est, en qualité de responsable de Services partagés Canada, investie par les dispositions des lois ou de leurs règlements mentionnées en regard de chaque poste. Le présent document remplace et annule tout arrêté de délégation antérieur.

Annexe

Poste	*Loi sur l'accès à l'information et Règlement*	*Loi sur la protection des renseignements personnels et Règlement*
Président	Autorité absolue	Autorité absolue
Première vice-présidente	Autorité absolue	Autorité absolue
Secrétaire ministérielle et chef de la protection des renseignements personnels	Autorité absolue	Autorité absolue
Directeur, Division de l'accès à l'information et de la protection de la vie privée	Autorité absolue	Autorité absolue
Directeurs adjoints, Opérations et Politique et gouvernance, Direction de l'accès à l'information et protection des renseignements personnels	Autorité absolue	Autorité absolue

Daté, à Ottawa, ce _____ jour de _____, 2020.

The Honourable Joyce Murray / L'honorable Joyce Murray
Minister of Digital Government and Head of Shared Services Canada/
Ministre du Gouvernement numérique et Responsable de Services partagés 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: 2020-04-01 to 2021-03-31

Part 1: Requests under the *Privacy Act*

	Number of requests
Received during the reporting period	59
Outstanding from the previous reporting period	3
Total	62
Closed during the reporting period	60
Carried over to the next reporting period	2

Part 2: Requests closed during the reporting period

2.1 Disposition and completion time

Disposition of requests	Completion time							
	1 to 15 Days	16 to 30 Days	31 to 60 Days	61 to 120 Days	121 to 180 Days	181 to 365 Days	More than 365 Days	Total
All disclosed	1	0	0	0	0	0	0	1
Disclosed in part	0	8	11	1	1	0	0	21
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	30	1	0	0	0	0	0	31
Request abandoned	7	0	0	0	0	0	0	7
Neither confirmed nor denied	0	0	0	0	0	0	0	0
Total	38	9	11	1	1	0	0	60

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)	6	24(b)	0
19(1)(d)	0	22(1)(c)	0	25	0
19(1)(e)	0	22(2)	0	26	19
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

Paper	Electronic	Other formats
0	22	0

2.5 Complexity

2.5.1 Relevant pages processed and disclosed

Number of pages processed	Number of pages disclosed	Number of requests
38,385	5,932	29

2.5.2 Relevant pages processed and disclosed by size of requests

Disposition	100 pages or less processed		101-500 pages processed		501-1,000 pages processed		1,001-5,000 pages processed		More than 5,000 pages processed	
	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed
All disclosed	1	5	0	0	0	0	0	0	0	0
Disclosed in part	4	132	7	607	2	232	6	2,911	2	2,045
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	7	0	0	0	0	0	0	0	0	0
Neither confirmed nor denied	0	0	0	0	0	0	0	0	0	0
Total	12	137	7	607	2	232	6	2,911	2	2,045

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	2	2
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	0	0	0	2	2

2.6 Closed requests

2.6.1 Number of requests closed within legislated timelines

	Requests closed within legislated timelines
Number of requests closed within legislated timelines	59
Percentage (%) of requests closed within legislated timelines	98.3

2.7 Deemed refusals

2.7.1 Reasons for not meeting legislative timelines

Number of requests closed past the statutory deadline	Principal reason			
	Interference with operations/ workload	External consultation	Internal consultation	Other
1	1	0	0	0

2.7.2 Requests closed beyond legislative timelines (including any extensions taken)

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	1	1
121 to 180 days	0	0	0
181 to 365 days	0	0	0
More than 365 days	0	0	0
Total	0	1	1

2.8 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

Number of requests where an extension was taken	15(a)(i) Interference with operations				15 (a)(ii) Consultation			15(b) Translation purposes or conversion
	Further review required to determine exemptions	Large volume of pages	Large volume of requests	Documents are difficult to obtain	Cabinet Confidence section (section 70)	External	Internal	
13	0	13	0	0	0	0	0	0

5.2 Length of extensions

Length of Extensions	15(a)(i) Interference with operations				15 (a)(ii) Consultation			15(b) Translation purposes or conversion
	Further review required to determine exemptions	Large volume of pages	Large volume of requests	Documents are difficult to obtain	Cabinet Confidence section (section 70)	External	Internal	
1 to 15 days	0	0	0	0	0	0	0	0
16 to 30 days	0	13	0	0	0	0	0	0
31 days or greater								0
Total	0	13	0	0	0	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

	Number of days required to complete consultation requests							
Recommendation	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

	Number of days required to complete consultation requests							
Recommendation	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

Part 7: Completion time for consultations on Cabinet Confidences

7.1 Requests with Legal Services

Number of Days	100 Pages or Less Processed		101-500 Pages Processed		501-1,000 Pages Processed		1,001-5,000 Pages Processed		More Than 5,000 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 the Privy Council Office

Number of Days	100 Pages or Less Processed		101-500 Pages Processed		501-1,000 Pages Processed		1,001-5,000 Pages Processed		More Than 5,000 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

9.1 Privacy Impact Assessments

Number of PIAs completed	1

9.2 Personal Information Banks

Personal information banks	Active	Created	Terminated	Modified
	6	1	0	0

Part 10: Material privacy breaches

Number of material privacy breaches reported to TBS	1
Number of material privacy breaches reported to OPC	1

Part 11: Resources related to the *Privacy Act*

11.1 Costs

Expenditure		Amount
Salaries		$456,108
Overtime		$0
Goods and services		$15,527
• Professional services contracts	$0	
• Other	$15,527	
Total		**$471,635**

11.2 Human Resources

Resources	Person-years dedicated to privacy activities
Full-time employees	5.500
Part-time and casual employees	0.208
Regional staff	0.000
Consultants and agency personnel	0.000
Students	0.000
Total	5.708
Note: Enter values to three decimal places.	