



National  
Defence

Défense  
nationale



CANADIAN  
ARMED FORCES

Annual Report to Parliament | 2019-2020

# Administration of the *Privacy Act*

Department of National Defence and the Canadian Armed Forces



# CONTENTS

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1.	Purpose of the <i>Privacy Act</i> .....	1
<b>2.</b>	<b>ACCESS TO INFORMATION AND PRIVACY AT NATIONAL DEFENCE .....</b>	<b>1</b>
2.1.	Mandate of National Defence .....	1
2.2.	National Defence Organization .....	2
2.3.	The Directorate of Access to Information and Privacy .....	3
<b>3.</b>	<b>HIGHLIGHTS OF THE STATISTICAL REPORT .....</b>	<b>5</b>
3.1.	Requests received .....	6
3.2.	Requests completed .....	7
3.3.	Consultations received and completed .....	9
<b>4.</b>	<b>COVID-19 IMPACTS TO PRIVACY OPERATIONS .....</b>	<b>9</b>
<b>5.</b>	<b>PRIVACY PROTECTION AND PERSONAL INFORMATION MANAGEMENT .....</b>	<b>10</b>
5.1.	Public Interest Disclosures .....	10
5.2.	Privacy Breaches .....	11
5.3.	Privacy Impact Assessments .....	11
<b>6.</b>	<b>COMPLAINTS, AUDITS AND REVIEWS .....</b>	<b>12</b>
6.1.	Complaints from the Office of the Privacy Commissioner .....	12
6.2.	Court Decisions .....	13
<b>7.</b>	<b>POLICIES AND PROCEDURES .....</b>	<b>13</b>
7.1.	Departmental Policies .....	13
<b>8.</b>	<b>TRAINING AND AWARENESS .....</b>	<b>14</b>
8.1.	ATIP training program .....	14
8.2.	Training and awareness activities .....	14
8.3.	Continuous Learning .....	15
<b>9.</b>	<b>INITIATIVES AND PROJECTS .....</b>	<b>15</b>
9.1.	On-Time Team .....	15
9.2.	Technological Improvements .....	16
9.3.	Litigation Support Team .....	16
<b>10.</b>	<b>MONITORING COMPLIANCE .....</b>	<b>16</b>
<b>11.</b>	<b>PRIVACY OPERATING COSTS .....</b>	<b>17</b>
	<b>ANNEX A: DESIGNATION ORDER .....</b>	<b>A-1</b>
	<b>ANNEX B: STATISTICAL REPORT ON THE <i>PRIVACY ACT</i> FOR 2019-2020 .....</b>	<b>B-1</b>
	<b>ANNEX C: SUPPLEMENTAL STATISTICAL REPORT ON THE <i>PRIVACY ACT</i> FOR 2019-2020 .....</b>	<b>C-1</b>

## 1. INTRODUCTION

The Department of National Defence and the Canadian Armed Forces are pleased to present to Parliament their annual report on the administration of the *Privacy Act*<sup>1</sup>. Section 72 of the Act requires the head of every federal government institution to submit an annual report to Parliament on its administration each financial year. This report describes National Defence activities that support compliance with the *Privacy Act* for the fiscal year (FY) commencing 1 April 2019 and ending 31 March 2020.

### 1.1. Purpose of the *Privacy Act*

The purpose of the *Privacy Act* is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.

These rights of protection and access are in accordance with the principles that individuals should have a right to know why their information is collected by the government, how it will be used, how long it will be kept and who will have access to it.

## 2. ACCESS TO INFORMATION AND PRIVACY AT NATIONAL DEFENCE

### 2.1. Mandate of National Defence

#### *Who we are*

The Department of National Defence (DND) and the Canadian Armed Forces (CAF) make up the largest federal government department. Under Canada's defence policy, the Defence Team will grow to over 125,000 personnel, including 71,500 Regular Force members, 30,000 Reserve Force members and 25,000 civilian employees.

#### *What we do*

DND and the CAF have complementary roles to play in providing advice and support to the Minister of National Defence, and implementing Government decisions regarding the defence of Canadian interests at home and abroad.

At any given time, the Government of Canada can call upon the CAF to undertake missions for the protection of Canada and Canadians and to maintain international peace and stability.

---

<sup>1</sup> <https://laws-lois.justice.gc.ca/eng/acts/P-21/>

Canada's defence policy presents a new strategic vision for defence: [Strong, Secure, Engaged](#).<sup>2</sup> This is a vision in which Canada is:

**Strong at home**, with a military ready and able to defend its sovereignty, and to assist in times of natural disaster, support search and rescue, or respond to other emergencies.

**Secure in North America**, active in a renewed defence partnership in the North American Aerospace Defense Command (NORAD) and with the United States to monitor and defend continental airspace and ocean areas.

**Engaged in the world**, with the Canadian Armed Forces doing its part in Canada's contributions to a more stable, peaceful world, including through peace support operations and peacekeeping.

The National Defence Act (NDA) establishes DND and the CAF as separate entities, operating within an integrated National Defence Headquarters as they pursue their primary responsibility of providing defence for Canada and Canadians.

## 2.2. National Defence Organization

### *Senior leadership*

The Governor General of Canada is the Commander-in-Chief of Canada. DND is headed by the Minister of National Defence. The Associate Minister of National Defence supports the Minister of National Defence. The Deputy Minister of National Defence is the Department's senior civil servant. The CAF are headed by the Chief of the Defence Staff, Canada's senior serving officer. These senior leaders each have different responsibilities:

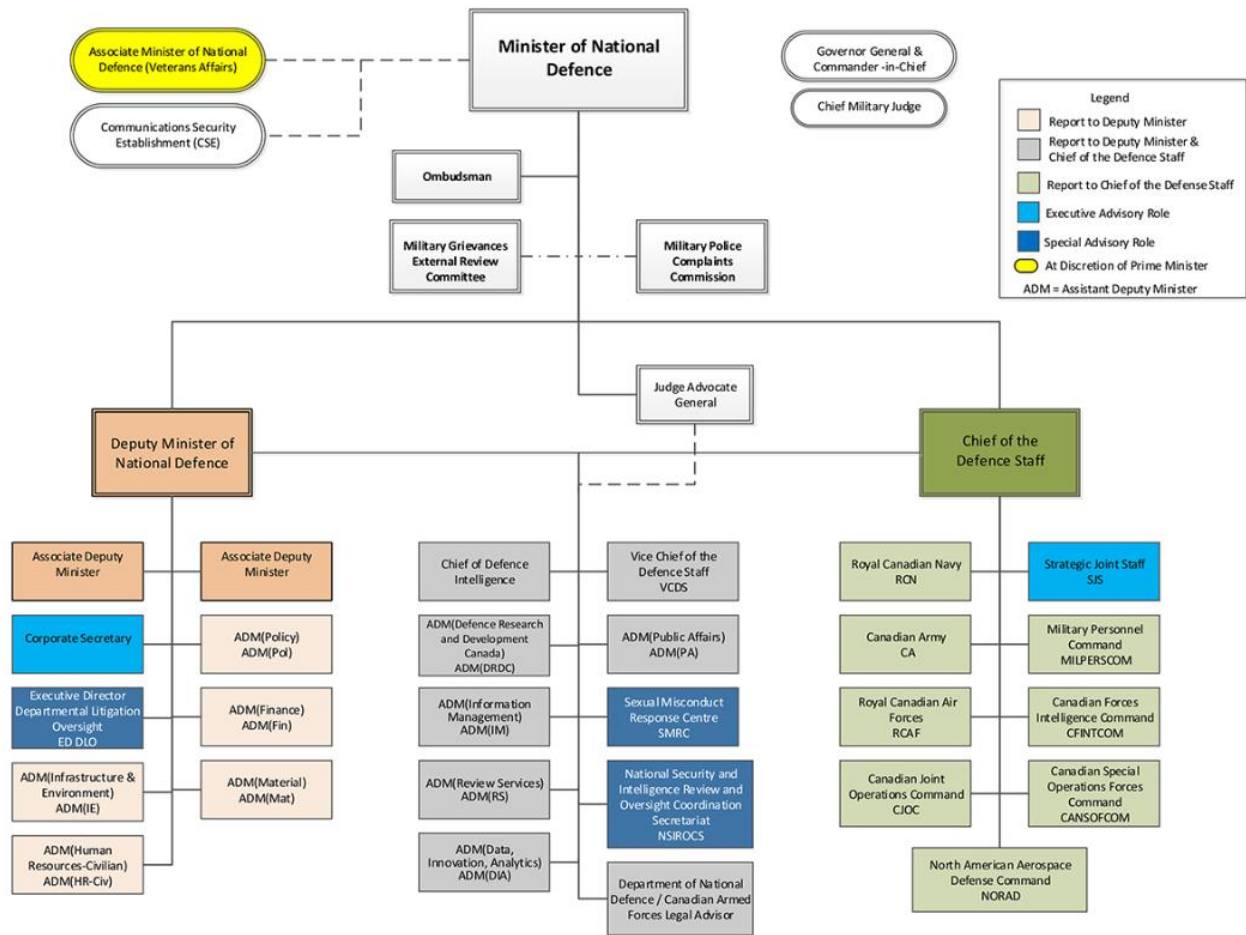
- The Governor General is responsible for appointing the Chief of the Defence Staff on the recommendation of the Prime Minister, awarding military honours, presenting colours to CAF regiments, approving new military badges and insignia, and signing commission scrolls;
- The Minister of National Defence presides over the Department and over all matters relating to national defence;
- The Associate Minister is also responsible for defence files, as mandated by the Prime Minister, with the specific priority of ensuring that CAF members have the equipment they need to do their jobs;
- The Deputy Minister is responsible for policy, resources, interdepartmental coordination and international defence relations; and
- The Chief of the Defence Staff is responsible for command, control and administration of the CAF, as well as military strategy, plans and requirements.

<sup>2</sup> [https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html?utm\\_source=dgpaapp&utm\\_medium=referral&utm\\_campaign=redirect](https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html?utm_source=dgpaapp&utm_medium=referral&utm_campaign=redirect)

## Defence Organization

The National Defence organizational structure is represented in the diagram below. Additional information about the National Defence organization is available [online](#).<sup>3</sup>

FIGURE 1: NATIONAL DEFENCE ORGANIZATION CHART



## 2.3. The Directorate of Access to Information and Privacy

### Delegation of Authority

In accordance with section 73(1) of the *Privacy Act*, a delegation of authority, signed by the Minister, designates the Deputy Minister, Corporate Secretary, Access to Information and Privacy (ATIP) Director, and ATIP Deputy Directors to exercise all powers and functions of the Minister, as the head of institution, under

<sup>3</sup> <https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html>

the Act. It also designates other specific powers and functions to employees within the Directorate Access to Information and Privacy (DAIP).

Under the authority of the Corporate Secretary, the ATIP Director administers and coordinates the *Access to Information Act* and the *Privacy Act*, and acts as the departmental ATIP Coordinator. In the administration of the Act, the ATIP Directorate seeks advice on legal, public affairs, policy, and operational security matters from other organizations and specialists as required.

A copy of the *Access to Information Act* and *Privacy Act* Designation Order is provided at ANNEX A.

### *The ATIP Directorate*

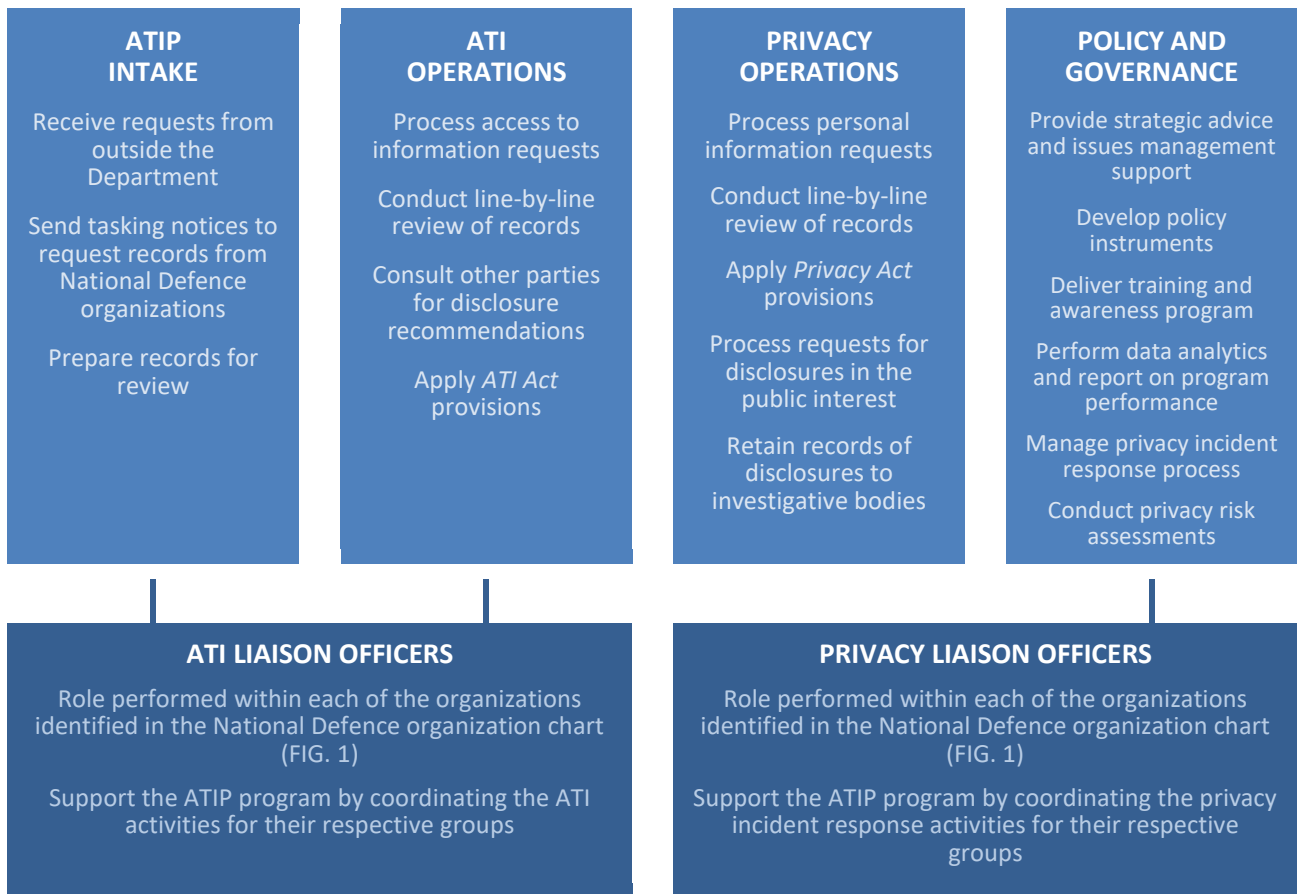
The ATIP Directorate is responsible for matters regarding access to information and privacy protection within the National Defence portfolio, except in the case of the following organizations: the Military Police Complaints Commission, the Military Grievances External Review Committee, the Office of the National Defence and Canadian Forces Ombudsman, the Office of the Chief Military Judge and the Director of Defence Counsel Services, and the Canadian Forces Morale and Welfare Services.

As a result of ATIP program review, the ATIP Directorate conducted an organization review and design exercise supported by Human Resources and staff which resulted in organizational changes aimed to increase efficiencies, build a robust support system and to streamline Access Operations. The Director Access to Information and Privacy was elevated to an Executive Director level position and a new Chief of Operations position was created to oversee all ATI Operations from intake to disclosure. The System Liaison Team was staffed with a Database Administrator to support case management and redaction software and a Corporate Services Manager position was created to ensure strengthened oversight of our financial and human resources.

The Chief of Operations position established a centralized leadership role which ensures consistency across teams, quality assurance activities for data and compliance to processes, tracking performance as well as monitoring for the identification of trends and horizontal issues. The ATIP Intake team, Systems Liaison Team and ATI Operations teams report to Chief of Operations. The Chief of Operations, Privacy Operations, Policy and Governance Team and the Chief of Staff report to the Executive Director.

The Directorate's ATIP program management workforce is divided functionally into four main areas, and supported by Defence organization liaison officers, as illustrated in the diagram at FIGURE 2.

FIGURE 2: NATIONAL DEFENCE ATIP OPERATIONAL WORKFORCE



The ATIP Directorate is supported by a Systems Liaison Team that maintains the ATIP application system and database, and a Business Management Office that is responsible for business planning, budgeting, human resources, physical security, and other administrative duties.

In response to a key National Defence priority, The ATIP Directorate maintained a Litigation Support Team. This unit performs an ATIP-like review of records in support of class action settlements such as the LBGT Class Action and the DND/CAF Sexual Misconduct Class Action settlements.

### 3. HIGHLIGHTS OF THE STATISTICAL REPORT

The statistical report at ANNEX B consists of data submitted by National Defence as part of Treasury Board Secretariat (TBS) annual collection of ATIP-related statistics. The following sections contain highlights, trends and an analysis of notable statistical data from a departmental perspective.

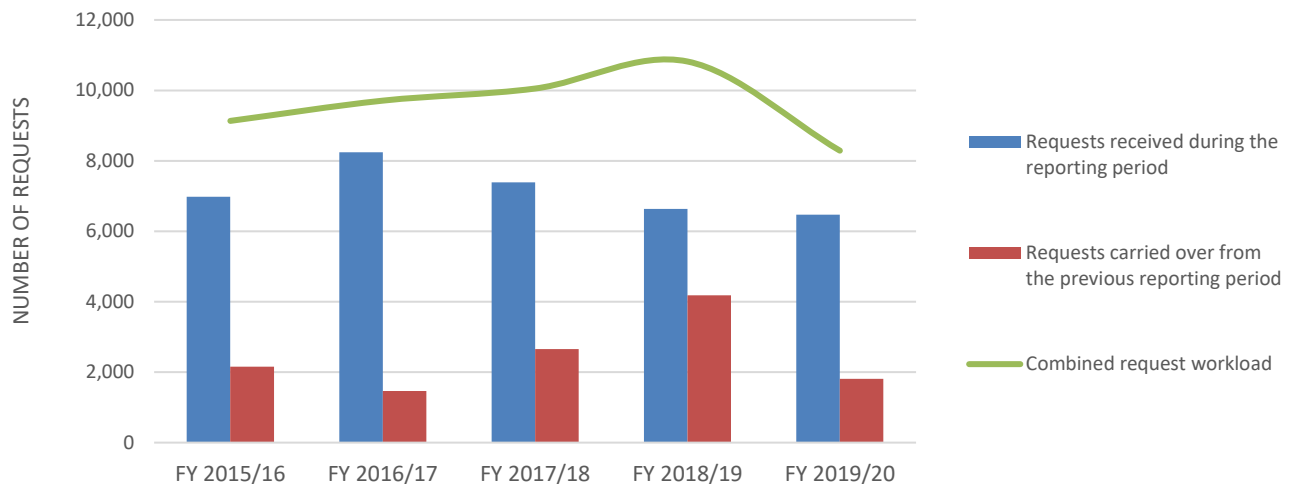
### 3.1. Requests received

During the reporting period, National Defence received 6,475 requests for personal information under the *Privacy Act* versus 6,637 in FY 2018-2019, representing a 2.4% decrease. This represents the third consecutive year of decreased requests for personal information and may be attributable to the implementation of the departmental initiative to pro-actively provide copies of health records to releasing CAF members that began in FY 2018-2019. Combined with 1814 files carried over from the previous reporting period the total workload of 8,289 requests is the lowest National Defence has experienced in over five years.

#### *Carry forward*

National Defence realized a significant 57% reduction in files carried forward into next FY. The number of requests carried over reduced from 4183 in FY 2018-19 to only 1814 requests this reporting period.

FIGURE 3: PRIVACY REQUEST WORKLOAD (LAST FIVE YEARS)



Of note, for more than a decade, National Defence has ranked in the top five federal institutions for the highest volume of personal information requests received according to annual statistics compiled by [TBS](#).<sup>4</sup>

A large portion of *Privacy Act* requests historically received by National Defence were applications from CAF members for their health and personnel records upon releasing from the Forces. As part of Canada's Defence Policy, the Canadian Forces Health Services group began pro-actively providing releasing CAF members with copies of their health records in FY 2018-2019. This initiative is aligned with the Government's commitment to transparency and has improved the transition experience for releasing CAF members to better prepare them

<sup>4</sup> <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/statistics-atip.html>

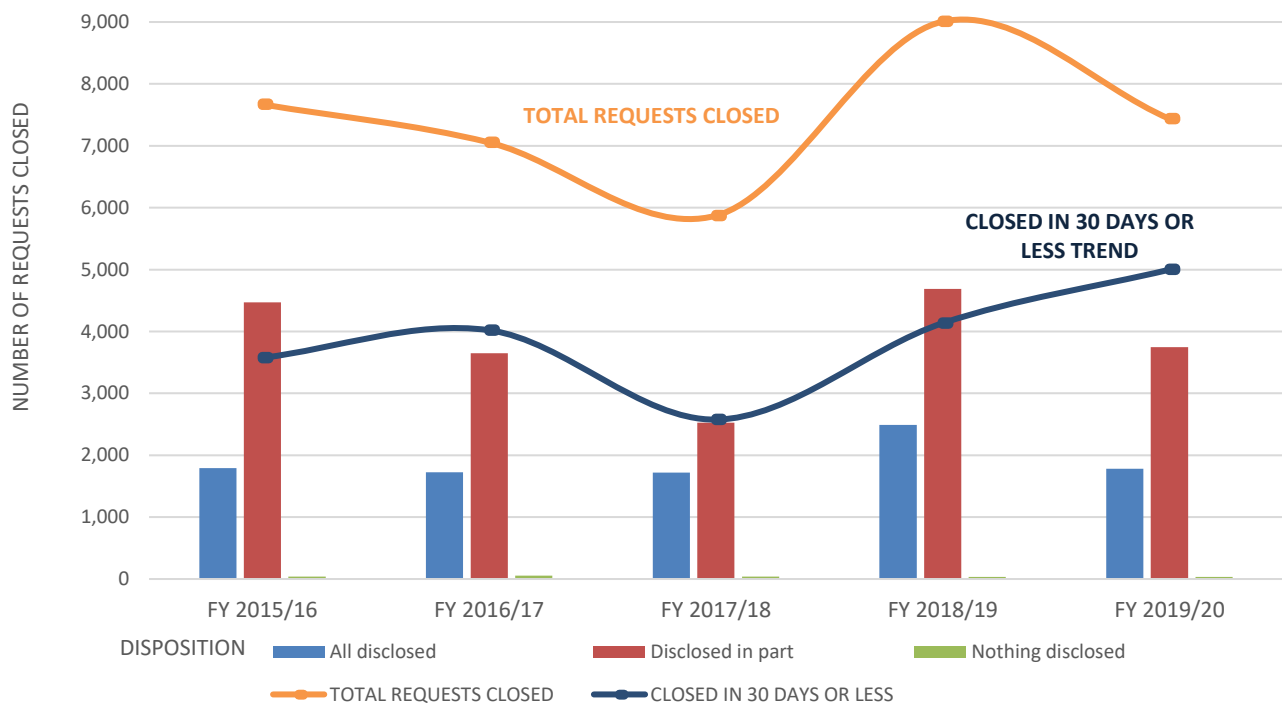


for the shift to civilian life and has also resulted in the reduction in the number of personal information requests received.

### 3.2. Requests completed

National Defence closed a total of 7,436 privacy requests during the reporting period. This represents 1570 fewer files closed (a 17.4% decrease) over the previous FY. While the number of requests closed has decreased, FIGURE 4 also demonstrates a significant increase in on-time performance.

FIGURE 4: DISPOSITION OF REQUESTS COMPLETED AND TOTAL REQUESTS CLOSED (LAST FIVE YEARS)



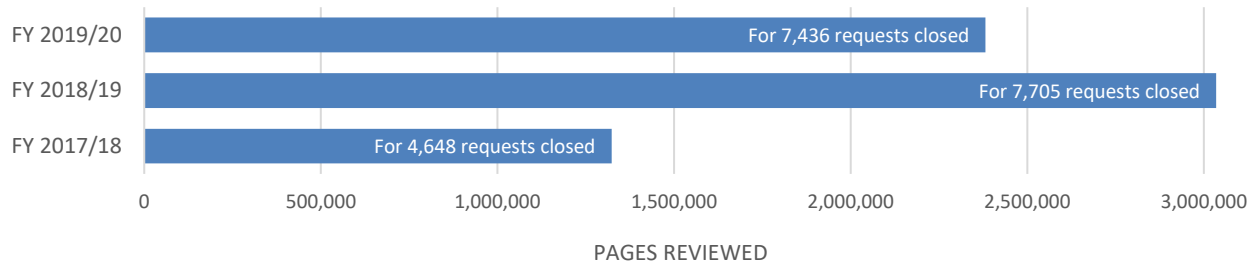
#### Pages reviewed

National Defence consistently processes the highest volume of pages in response to personal information requests when compared to other federal government institutions.<sup>5</sup>

A total of 2,381,632 pages were reviewed this reporting period. This represents a 21.5% reduction in pages processed from FY 2018-2019. As shown in FIGURES 4 & 6, National Defence noted a significant increase in on-time performance.

<sup>5</sup> <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/statistics-atip.html>

FIGURE 5: NUMBER OF PAGES REVIEWED FOR REQUESTS CLOSED, WHERE RECORDS EXISTED (LAST THREE YEARS)



The number of pages reviewed represents the total pages processed for closed requests and does not include the number of pages processed for requests reviewed in the current FY that were carried over into the next reporting period.

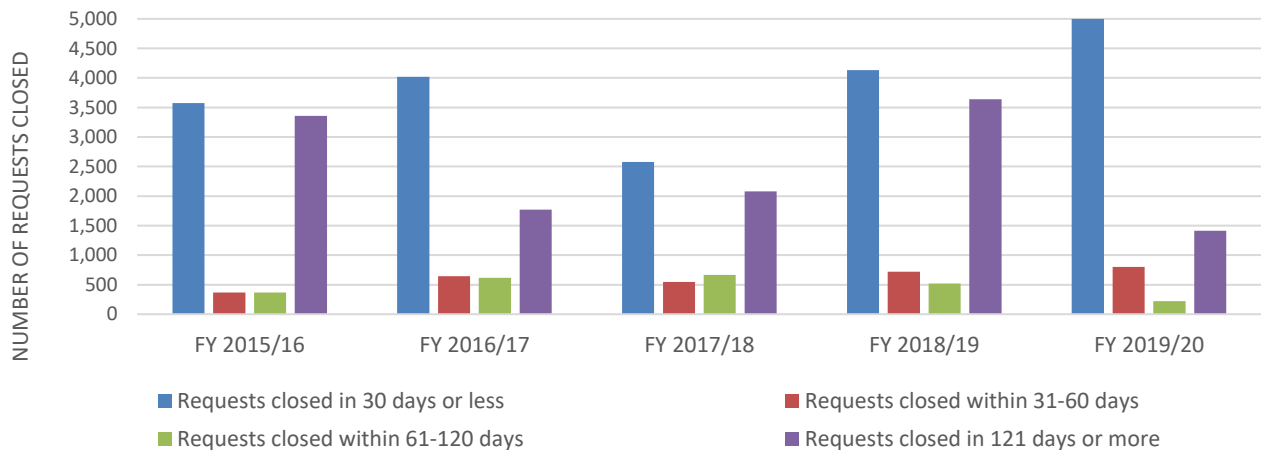
### Exemptions and exclusions

Consistent with previous reporting periods, section 26 of the *Privacy Act* was the most frequently invoked exemption and was applied in 3,733 requests. This section of the Act protects personal information of individuals other than the requester.

### Completion time

As demonstrated in FIGURE 6, National Defence noted a significant improvement in on-time compliance for a third consecutive year. Defence closed 4,998 requests within 30 days which represents 67% of the total volume of requests closed. This represents a 21% increase of files closed within 30 days compared to the last reporting period. Additionally, the number of files closed in excess of 121 days decreased significantly from 3637 files in FY 2018-19 to 1412 during this reporting period.

FIGURE 6: TIME TO COMPLETE REQUESTS (LAST FIVE YEARS)



Files closed beyond 30 days were not necessarily late as legal extensions may have been applied.

### *On-time compliance*

National Defence noted a 26% improvement in on-time compliance over the previous reporting period. A total of 5,542 requests (75%) were closed within statutory deadlines in FY 2019-2020.

Improvements in compliance can be attributed to the establishment of a dedicated team focused on closing files within statutory deadlines. National Defence noted a 12% increase in files closed within 31-60 days over the previous reporting period.

Workload continued to be the most common reason for deemed refusal, cited for nearly 64% of requests closed late during the reporting period. Some factors affecting performance and deemed refusal rates include:

- Impacts to productivity and efficiency resulting from staffing challenges. There continues to be staff turnover at all levels due to a competitive job market. New employees require a learning and adjustment period to realize performance potential. The hiring and training of new employees also created additional workload for ATIP management and support services.

## **3.3. Consultations received and completed**

During the reporting period, Defence received six requests for consultation, three were from other Government of Canada institutions and three were from other organizations.

Four of the six consultations received were closed during the reporting period.

## **4. COVID-19 IMPACTS TO PRIVACY OPERATIONS**

### *Operation LASER*

Operation LASER<sup>6</sup> is the Canadian Armed Forces' response to a worldwide pandemic situation.

During Operation LASER, the CAF implemented certain measures on their personnel and Department of National Defence (DND) employees to reduce the impacts of a pandemic situation. These measures were implemented in order to maintain operational capabilities and readiness to support Government of Canada objectives and requests for assistance.

On March 13, 2020, DND/CAF initiated its Business Continuity Plan (BCP) in response to the evolving COVID-19 pandemic. A limited number of employees across the Department designated as essential services were

---

<sup>6</sup> <https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/laser.html>

required to work at various office locations; while others were equipped with government supplied laptops, and established connectivity to the Defence Wide Virtual Private Network (VPN) to enable them to work remotely from home.

### *ATIP Operations*

The ATIP Operations teams assumed a telework posture. VPN access was initially limited to ensure essential DND/CAF services could be performed. In addition to limited VPN capability, the majority of ATI work requires access to secure networks to review and redact information which significantly impacted ATI Operations. While the Privacy Operations team has the ability to process files remotely; VPN connectivity was limited in the initial BCP period which impacted Privacy Operations.

National Defence took a proactive approach to managing COVID-19 impacts to ATIP program delivery. Following TBS Guidance, applicants were notified of reduced capacity and the expectation of delays due to the exceptional circumstances. Individual applicants were each contacted directly to seek their consent to place request files on hold.

The COVID-19 supplemental statistical report at ANNEX C represents National Defence impacts to ATI Operations. A total of 175 requests made under the *Privacy Act* were received during the two-week COVID-19 period in March 2020 during FY 2019-2020.

### *Policy & Governance Team*

The ATIP Policy & Governance (P&G) team provides strategic advice and support to management. This includes privacy advisory services to the department for matters relating to COVID-19 activities including the collection, use and disclosure of personal information relating to COVID-19 tracking. The P&G team assumed a telework posture with limited VPN connectivity during the initial COVID BCP period.

## **5. PRIVACY PROTECTION AND PERSONAL INFORMATION MANAGEMENT**

### **5.1. Public Interest Disclosures**

Paragraph 8(2)(m) of the *Privacy Act* permits the disclosure of personal information, without the consent of the individual to whom it relates, where the public interest in disclosure clearly outweighs any invasion of privacy that could result, or where the disclosure would clearly benefit the individual to whom the information relates.

During the reporting period, 62 disclosures of personal information were made in accordance with paragraph 8(2)(m). These public interest disclosures included information regarding Boards of Inquiry or Summary Investigations into the death or serious injury of a CAF member; others related to disclosures providing

information in CAF medical records, personnel records or military police reports. In all cases, the information was disclosed to the CAF member's family or representative.

For each of the 62 disclosures made in the public interest during FY 2019-2020, the Office of the Privacy Commissioner (OPC) was notified in advance of each release.

## 5.2. Privacy Breaches

Privacy rights are a matter of ongoing public concern. In respect of sections 4 to 8 of the *Privacy Act*, which govern personal information management, the ATIP Directorate received 136 complaints regarding contravention of one or more of these provisions. The ATIP Directorate's Privacy Incident Management team reviewed and resolved 117 complaints alleging a breach of privacy, of which 66 complaints were deemed to be well-founded.

### *Material Privacy Breaches*

TBS defines a material privacy breach as one that involves sensitive personal information and could reasonably be expected to cause injury or harm to the individual, and/or involves a large number of affected individuals. National Defence did not report any material privacy breaches this reporting period.

## 5.3. Privacy Impact Assessments

National Defence collects, uses and discloses personal information in the delivery of mandated programs and services. In accordance with TB policy, the DND and the CAF undertake privacy impact assessments (PIA) to evaluate privacy impacts in the administration of these activities. A PIA provides a framework to identify the extent to which proposals comply with the *Privacy Act* and applicable privacy policies, assist program officials in avoiding or mitigating privacy risks, and promote informed program and system design choices.

National Defence completed<sup>7</sup> two PIAs during FY 2019-2020 described below:

- In support of Operation HONOUR, the Sexual Misconduct Reporting Centre (SMRC) was created in 2015 to provide confidential support to active Canadian Armed Forces (CAF) members affected by harmful and inappropriate sexual behavior and to help them make informed choices on available services and resources to meet their individual needs.
- The ATIP program PIA assesses the risks related to the collection, use, safeguarding, retention, and disclosure of personal information collected in support of the Directorate's three business lines - processing requests under the Access to Information Act and the Privacy Act, as well as privacy incident management. This PIA also assessed the privacy management framework of DND, including the existing privacy policies and related activities.

---

<sup>7</sup> Completed PIAs must be submitted to the Treasury Board of Canada Secretariat, as well as to the Office of the Privacy Commissioner.

In addition, DAIP continues to provide ongoing privacy advisory services to National Defence organizations assessing risks to personal information used in the administration of Defence programs.

## 6. COMPLAINTS, AUDITS AND REVIEWS

### 6.1. Complaints from the Office of the Privacy Commissioner

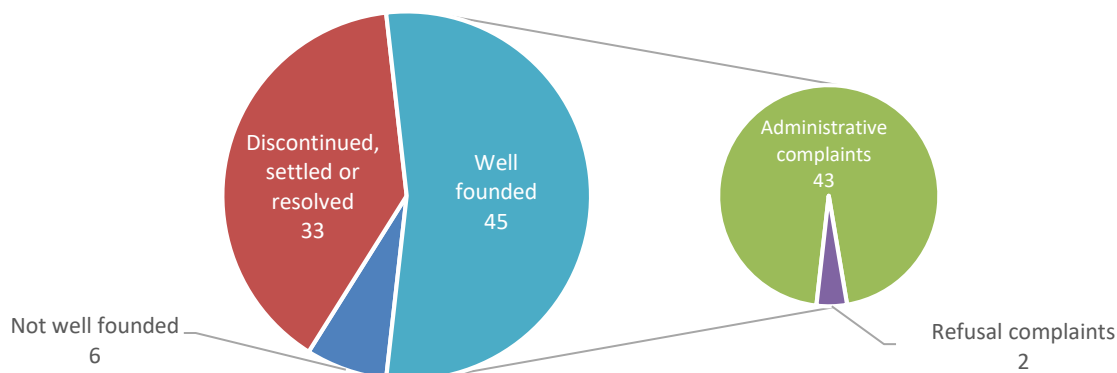
In FY 2019-20, National Defence received a total of 22 complaints from the Office of the Privacy Commissioner (OPC), representing less than one percent of all requests closed during the reporting period.

Further to Part 8 of the Statistical Report, which notes complaints received and closed:

- Section 31: When the OPC gives formal notice of their intention to investigate a complaint regarding the processing of a request under the Act. Defence received 22 such notices during FY 2019-20 as compared to 77 such notices during FY 2018/19 (a 71% decrease from the last reporting period).
- Section 33: When the OPC requests further representations from institutions pursuant to an ongoing complaint investigation. Defence received 50 such notices during FY 2019-20 in comparison to zero such notices in the previous reporting period.
- Section 35: When the OPC issues a findings report for a well-founded complaint upon conclusion of an investigation. During the reporting period, 45 complaints were found to have merit. Note that these complaints are not necessarily from the 22 complaints received during the reporting period.

The 45 well-founded determinations represent 54% of all findings issued in FY 2019-2020. The majority of these complaints – 43 – were administrative in nature (about delays and time extensions) and two were refusal complaints (regarding application of exemptions or possible missing records). FIGURE 7 illustrates the reasons for complaints that had findings issued during the reporting period.

FIGURE 7: REASONS FOR COMPLAINT (FY 2019-2020)



## 6.2. Court Decisions

In FY 2019-20, the ATIP Directorate received one application for judicial review further to a well-founded complaint issued by the Office of the Privacy Commissioner. The complaint related to a delay wherein DND was in “deemed refusal”. Ultimately, the requester discontinued the application for judicial review and the Notice of Discontinuation was received by DND in January 2020.

## 7. POLICIES AND PROCEDURES

### 7.1. Departmental Policies

DND/CAF corporate administrative direction is set out in the comprehensive collection of Defence Administrative Orders and Directives (DAOD) that are issued under the authority of the Deputy Minister and the Chief of the Defence Staff.

During the reporting period, the ATIP Directorate finalized the revision of the suite of ATIP DAOD including:

- the policy on Administration of the *Privacy Act*,
- the directives on:
  - Privacy Act Requests,
  - Personal Information Management,
  - Privacy Incident Management,
  - Privacy Impact Assessments, and
  - Disclosure of Personal Information.

These policy instruments describe authorities and responsibilities to uphold legal requirements under the *Privacy Act*. To ensure information is accessible by all, the DAOD are published on the Defence Network for DND/CAF employees and members and are available on the internet to the general public.

#### *Internal procedures*

The ATIP Directorate continues to review and update procedures for processing personal information requests and managing privacy incidents, to document process improvements, and to ensure alignment with TB policies and directives. This reporting period, a Privacy Operations Directive was created and implemented. It is a tool to support analysts at all levels during the review of records and it ensures consistency across the Privacy Operations teams.

Additionally, the ATIP Directorate formalized a Standard Operating Procedure (SOP) describing the application of extensions under Section 15 to assure consistency and compliance when applying extensions. The SOP includes outlines of the reason(s) that an extension can be taken in accordance with the Privacy Act and describes how to capture the reason to support reporting requirements.

## 8. TRAINING AND AWARENESS

### 8.1. ATIP training program

Departmental ATIP training remained consistent during this reporting period. The previously reported three-pronged training approach was maintained, where Directorate training resources delivered the following training sessions to DND civilian and CAF military members with specific emphasis on those staff with ATIP responsibilities:

- Introductory courses (General ATIP or Privacy Fundamentals);
- Advanced courses (General ATIP or organization-specific content); and,
- ATIP awareness and engagement activities with the various branches and divisions.

Regional training sessions at Canadian Forces Bases Esquimalt, Edmonton, Cold Lake, Gagetown, Greenwood, Halifax, Shearwater, Kingston and Borden were also delivered during this reporting period.

### 8.2. Training and awareness activities

A total of 87 face-to-face training sessions were delivered to approximately 1,559 Defence employees and CAF members on the administration of both the *ATI Act* and *Privacy Act*, as well as on appropriate management of personal information under the control of the institution. These training sessions were provided through participation in ATIP 101 (introductory) sessions, ATIP 201 (advanced) sessions, GCDOCS privacy-focused training, and targeted training sessions for specific Defence organizations. Most training sessions were delivered by the ATIP Directorate staff in person or through video teleconference technologies, however some organizations conducted their own courses and one-on-one sessions. An example of organizations conducting their own training sessions included the 3 training events provided by the Canadian Forces Health Services group that covered a variety of Privacy topics – for a total of 135 persons trained. Defence employees and CAF members were also encouraged to take the Access to Information and Privacy Fundamentals course offered through the Canada School of Public Service.

In keeping with promoting awareness, the ATIP Directorate employees also provided guidance to third parties and requesters on the requirements of the *Access to Information Act* and the *Privacy Act*, TB policies and directives, and associated institutional procedures as required.

#### *Integrated privacy training*

The ATIP Directorate continued to collaborate on program-specific training offered by other Defence organizations to integrate supporting content on privacy protection concepts and personal information management practices. During FY 2019-2020, the ATIP Directorate participated in the GCDOCS on-boarding for information management specialists.



### *Canadian Forces Health Services training*

The Canadian Forces Health Services (CFHS) operates a privacy office that is responsible for providing advice and support to the CFHS Group on policies and activities that involve personal health information. In accordance with their mandate, the CHFS privacy office maintains training modules to educate staff on the principles of “Privacy, Confidentiality and Security” to support appropriate use of the Canadian Forces Health Information System.

During this reporting period, members of CFHS Group completed these modules and over 135 of their staff attended training offered specifically to the CFHS organization.

## **8.3. Continuous Learning**

As a result of the ATIP program review undertaken in 2017, the ATIP Directorate is fully committed to supporting the development and continuous learning for ATIP analysts. During the current reporting period, National Defence participated in a pilot project with several other government departments; *Programme de formation professionnelle en intégration en emploi des analystes fédéraux en AIPRP – 1e édition*<sup>8</sup> course hosted by *L’Association des professionnels en accès à l’information et en protection de la vie privée*<sup>9</sup> (AAPI). This course provides an overview of ATIP legislative considerations and is targeted at junior analysts. Four (4) ATIP analysts from National Defence participated. Additionally, a full day of professional development training was provided to all ATIP staff. The topics included personal information management, privacy incident management, the use of action codes in the ATIP case management and review of cabinet confidences.

## **9. INITIATIVES AND PROJECTS**

### **9.1. On-Time Team**

Privacy Operations implemented a dedicated team to focus on compliance and processing requests within the 30-day legislated timeframe. Additionally, this team focused on applying legitimate extensions pursuant to Section 15 of the Act. These focused efforts realized an impressive increase in on-time compliance of 75% compared to 49% in the previous year.

---

<sup>8</sup> Professional training program for new or junior federal ATIP analysts – 1<sup>st</sup> edition

<sup>9</sup> The Association of Access to Information and Privacy Protection Professionals

## 9.2. Technological Improvements

### *Privacy Operations Telework*

DAIP trialed the ability to review and redact privacy requests remotely during this reporting period. The trial period was successful and consequently, when the COVID-19 business continuity posture was implemented, many of the initial challenges associated with establishing a telework environment had been resolved.

### *New Case Management Solution*

DAIP is developing an innovative case management system to better manage the ATIP related activities outside of formal ATIP requests. This new case management system will improve tracking and trend analysis for governance and compliance activities such as: the provision of advisory services pertaining to the Access to Information and Privacy Acts, Privacy Incident Management, Privacy Impact Assessment development, managing and tracking legal matters and Personal Information Disclosures. It also includes features to maintain Personal Information Banks and Info Source management in a more automated manner.

## 9.3. Litigation Support Team

To support a key National Defence priority, DAIP maintained a Litigation Support Team. The LGBT Class Action occurred during FY 2019-20 to apologize for discrimination conducted against the LGBT community. The Litigation Support Team reviewed 464 files providing direct support the Departmental Litigation Oversight team.

## 10. MONITORING COMPLIANCE

DAIP regularly monitors and reports on a number of ATIP metrics. In FY 2019-2020, the Departmental ATIP Performance Dashboard was refined to provide better overall awareness to Defence leadership on ATIP performance and metrics. In addition, the Department continues to receive on-demand statistical reports and performance compared to previous fiscal years to identify trends. This monitoring allows the ATIP Directorate to track ATIP performance across the Department to identify potential areas for process improvements.

Currently, the time to process requests for correction of personal information is not formally monitored as this number is regularly very low. In FY 2019-2020, the ATIP Directorate received only one request for correction.

## 11. PRIVACY OPERATING COSTS

### *Costs*

The annual cost to administer the National Defence privacy program increased by 15 percent to approximately \$3,756,410 FY 2019-2020.

### *Human Resources*

During FY 2019-2020, an equivalent of 46.26 full-time employees were dedicated to administering the Privacy Act. For additional information refer to section 11 in Annex B.

## ANNEX A: DESIGNATION ORDER

### National Defence and the Canadian Armed Forces

#### *Access to Information Act and Privacy Act Designation Order*

1. Pursuant to section 73 of the *Access to Information Act* and the *Privacy Act*, the Minister of National Defence, as the head of a government institution under these Acts, hereby designates the persons holding the following positions, or the persons occupying those positions on an acting basis, to exercise or perform all of the powers, duties and functions of the head of a government institution under these Acts:

- (a) the Deputy Minister;
- (b) the Corporate Secretary;
- (c) the Director Access to Information and Privacy; and
- (d) Deputy Directors Access to Information and Privacy.

2. Pursuant to section 73 of the above-mentioned Acts, the Minister also designates the following:

(a) those persons holding the position of Access Team Leader, or the persons occupying this position on an acting basis, to exercise or perform the powers, duties and functions in respect of:

- The application of the following provisions under the *Access to Information Act*: section 9; subsections 11(2), 11(3), 11(4), 11(5), 11(6); sections 19, 20, 23 and 24; subsections 27(1) and 27(4); paragraph 28(1)(b), subsections 28(2) and 28(4); and
- The response to requests made under the *Access to Information Act* if no records exist.

(b) those persons holding the position of Privacy Team Leader, or the persons occupying this position on an acting basis, to exercise or perform any of the powers, duties and functions of the head of an institution under the *Privacy Act*, other than under sub-paragraphs 8(2)(j) and 8(2)(m); and

(c) those persons holding the position of Privacy Senior Analyst, or the persons occupying this position on an acting basis, to exercise or perform the powers and duties in respect of the application of section 26 of the *Privacy Act*.

### Défense nationale et les Forces armées canadiennes

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

1. En vertu de l'article 73 de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, le ministre de la Défense nationale, à titre de responsable d'une institution fédérale aux termes desdites lois, délègue par les présentes l'autorité d'exercer les attributions d'un responsable d'une institution fédérale que lui confèrent les lois en question aux titulaires des postes indiqués ci-après, ou aux personnes occupant ces postes à titre intérimaire :

- (a) le sous-ministre;
- (b) le Secrétaire général;
- (c) le Directeur – Accès à l'information et protection des renseignements personnels;
- (d) les Directeurs adjoints – Accès à l'information et protection des renseignements personnels.

2. En vertu de l'article 73 des lois susmentionnées, le ministre délègue aussi :

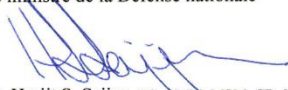
(a) aux titulaires d'un poste de chef d'équipe de l'accès à l'information, ou aux personnes occupant un tel poste à titre intérimaire, l'autorité d'exercer les attributions relatives à ce qui suit :

- L'application de certaines dispositions de la *Loi sur l'accès à l'information*, à savoir l'article 9; les paragraphes 11(2), 11(3), 11(4), 11(5) et 11(6); les articles 19, 20, 23 et 24; les paragraphes 27(1) et 27(4); l'alinéa 28(1)b), et les paragraphes 28(2) et 28(4);
- La réponse fournie aux demandes présentées en vertu de la *Loi sur l'accès à l'information*, lorsqu'il n'existe aucun dossier.

(b) aux titulaires d'un poste de chef d'équipe des renseignements personnels, ou aux personnes occupant un tel poste à titre intérimaire, l'autorité d'exercer les attributions du responsable d'une institution fédérale aux termes de la *Loi sur la protection des renseignements personnels*, sauf celles prévues aux alinéas 8(2)j) et m);

(c) aux titulaires d'un poste d'analyste principal, ou aux personnes occupant ces postes à titre intérimaire, l'autorité d'exercer les attributions relatives à l'application de l'article 26 de la *Loi sur la protection des renseignements personnels*.

Le ministre de la Défense nationale



The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

Minister of National Defence

Date: **JAN 12 2016**

**ANNEX B: STATISTICAL REPORT ON THE *PRIVACY ACT* FOR 2019-2020****Statistical Report on the *Privacy Act***Name of institution National DefenceReporting period: 2019-04-01 to 2020-03-31**Section 1: Requests Under the *Privacy Act***

	Number of Requests
Received during reporting period	6475
Outstanding from previous reporting period	1814
<b>Total</b>	<b>8289</b>
Closed during reporting period	7436
Carried over to next reporting period	853

**Section 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	456	874	202	34	13	108	96	1783
Disclosed in part	165	1701	537	167	95	527	555	3747
All exempted	22	10	2	0	1	0	0	35
All excluded	0	0	0	0	0	0	0	0
No records exist	1163	137	46	16	3	3	1	1369
Request abandoned	421	48	16	6	1	4	5	501
Request denied	1	0	0	0	0	0	0	1
<b>Total</b>	<b>2228</b>	<b>2770</b>	<b>803</b>	<b>223</b>	<b>113</b>	<b>642</b>	<b>657</b>	<b>7436</b>

## 2.2 Exemptions

Section	Number of Requests	Section	Number of Requests	Section	Number of Requests
18(2)	0	22(1)(a)(i)	121	23(a)	0
19(1)(a)	2	22(1)(a)(ii)	0	23(b)	0
19(1)(b)	0	22(1)(a)(iii)	0	24(a)	0
19(1)(c)	17	22(1)(b)	13	24(b)	0
19(1)(d)	10	22(1)(c)	0	25	1
19(1)(e)	0	22(2)	0	26	3733
19(1)(f)	0	22.1	1	27	99
20	0	22.2	1	27.1	0
21	25	22.3	1	28	2
		22.4	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)	1	70.1	0

## 2.4 Format of information released

Paper	Electronic	Other
861	4669	0

## 2.5 Complexity

### 2.5.1 Relevant pages processed and disclosed

Number of Pages Processed	Number of Pages Disclosed	Number of Requests
2381632	2286169	6067

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	1132	20767	339	83881	194	133523	118	146732	0	0
Disclosed in part	879	43260	1436	414279	817	572148	613	862964	2	8615
All exempt	35	0	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0	0	0
Request abandoned	499	0	2	0	0	0	0	0	0	0
Neither confirmed nor denied	1	0	0	0	0	0	0	0	0	0
<b>Total</b>	<b>2546</b>	<b>64027</b>	<b>1777</b>	<b>498160</b>	<b>1011</b>	<b>705671</b>	<b>731</b>	<b>1009696</b>	<b>2</b>	<b>8615</b>

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	9	6	0	3	18
All exempt	0	2	0	0	2
All excluded	0	0	0	0	0
Request abandoned	0	1	0	0	1
Neither confirmed nor denied	0	0	0	0	0
<b>Total</b>	<b>9</b>	<b>9</b>	<b>0</b>	<b>3</b>	<b>21</b>

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	5542
Percentage of requests closed within legislated timelines (%)	75%

## 2.7 Deemed refusals

### 2.7.1 Reasons for not meeting legislated timelines

Number of Requests Closed Past the Legislated Timelines	Principal Reason			
	Interference with Operations / Workload	External Consultation	Internal Consultation	Other
1894	1208	0	0	686

### 2.7.2 Requests closed beyond legislated timelines (including any extension taken)

Number of Days Past Legislated Timelines	Number of Requests Past Legislated Timeline Where No Extension Was Taken	Number of Requests Past Legislated Timelines Where an Extension Was Taken	Total
1 to 15 days	165	11	176
16 to 30 days	122	9	131
31 to 60 days	109	1	110
61 to 120 days	132	4	136
121 to 180 days	81	2	83
181 to 365 days	897	6	903
More than 365 days	355	0	355
<b>Total</b>	<b>1861</b>	<b>33</b>	<b>1894</b>

## 2.8 Requests for translation

Translation Requests	Accepted	Refused	Total
English to French	0	0	0
French to English	0	0	0
<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

## Section 3: Disclosures Under Subsections 8(2) and 8(5)

Paragraph 8(2)(e)	Paragraph 8(2)(m)	Subsection 8(5)	Total
186	62	62	310

## Section 4: Requests for Correction of Personal Information and Notations

Disposition for Correction Requests Received	Number
Notations attached	0
Requests for correction accepted	1
<b>Total</b>	<b>1</b>



**Section 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			
	Further review required to determine exemptions	Large volume of pages	Large volume of requests	Documents are difficult to obtain	Cabinet Confidence (Section 70)	External	Internal	15(b) Translation purposes or conversion
401	0	5	395	1	0	0	0	0

**5.2 Length of extensions**

Length of Extensions	15(a)(i) Interference with operations					15 (a)(ii) Consultation		
	Further review required to determine exemptions	Large volume of pages	Large volume of requests	Documents are difficult to obtain	Cabinet Confidence (Section 70)	External	Internal	15(b) Translation purposes or conversion
1 to 15 days	0	0	0	0		0	0	0
16 to 30 days	0	5	395	1		0	0	0
31 days or greater								0
Total	0	5	395	1		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	3	139	3	7
Outstanding from the previous reporting period	0	0	0	0
Total	3	139	3	7
Closed during the reporting period	2	62	2	2
Pending at the end of the reporting period	1	77	1	5

**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	1	0	0	0	0	0	0	1
Disclosed in part	0	0	1	0	0	0	0	1
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
<b>Total</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>

**6.3 Recommendations and completion time for consultations received from other**

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	1	1	0	0	0	0	0	2
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
<b>Total</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>

**Section 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
365	0	0	0	0	0	0	0	0	0	0
<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

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
365	0	0	0	0	0	0	0	0	0	0
<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

**Section 8: Complaints and Investigations Notices Received**

Section 31	Section 33	Section 35	Court action	Total
22	50	45	1	118

**Section 9: Privacy Impact Assessments (PIAs)**

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

9.2 Personal Information Banks

Personal Information Banks	Active	Created	Terminated	Modified
	104	0	0	1

**Section 10: Material Privacy Breaches**

Number of material privacy breaches reported to TBS	0
Number of material privacy breaches reported to OPC	0

## Section 11: Resources Related to the *Privacy Act*

### 11.1 Costs

Expenditures		Amount
Salaries		\$2,875,818
Overtime		\$9,289
Goods and Services		\$871,303
• Professional services contracts	\$594,397	
• Other	\$276,906	
<b>Total</b>		<b>\$3,756,410</b>

### 11.2 Human Resources

Resources	Person Years Dedicated to Privacy Activities
Full-time employees	41.88
Part-time and casual employees	0.12
Regional staff	0.00
Consultants and agency personnel	3.13
Students	1.13
<b>Total</b>	<b>46.26</b>

Note: Enter values to two decimal places.

## ANNEX C: SUPPLEMENTAL STATISTICAL REPORT ON THE *PRIVACY ACT* FOR 2019-2020

### Supplemental Statistical Report on the *Privacy Act*

The following table reports the total number of formal requests received during two periods; 2019-04-01 to 2020-03-13 and 2020-03-14 to 2020-03-31.

**Table 4 – Requests Received**

		Column (Col.) 1
		Number of requests
Row 1	Received from 2019-04-01 to 2020-03-13	6300
Row 2	Received from 2020-03-14 to 2020-03-31	175
Row 3	<b>Total<sup>1</sup></b>	<b>6475</b>

<sup>1</sup> – Total for Row 3 should equal the total in the Privacy Statistical Report Section 1.1 Row 1

The following table reports the total number of requests closed within the legislated timelines and the number of closed requests that were deemed refusals during two periods 2019-04-01 to 2020-03-13 and 2020-03-14 to 2020-03-31.

**Table 5 – Requests Closed**

		Col. 1	Col. 2
		Number of requests closed within the legislated timelines	Number of requests closed past the legislated timelines
Row 1	Received from 2019-04-01 to 2020-03-13 and outstanding from previous reporting periods	5512	1884
Row 2	Received from 2020-03-14 to 2020-03-31	30	10
Row 3	<b>Total<sup>2</sup></b>	<b>5542</b>	<b>1894</b>

<sup>2</sup> – Total for Row 3 Col. 1 should equal the total in the Privacy Statistical Report Section 2.6.1 Row 1 – Total for Row 3 Col. 2 should equal the total in the Privacy Statistical Report Section 2.7.1. Col. 1 Row 1

The following table reports the total number of requests carried over during two periods; 2019-04-01 to 2020-03-13 and 2020-03-14 to 2020-03-31.

**Table 6– Requests Carried Over**

		Col. 1
		Number of requests
Row 1	Requests from 2019-04-01 to 2020-03-13 and outstanding from previous reporting period that were carried over to the 2020-2021 reporting period	782
Row 2	Requests from 2020-03-14 to 2020-03-31 that were carried over to the 2020-2021 reporting period	71
Row 3	<b>Total<sup>3</sup></b>	<b>853</b>

<sup>3</sup> – Total for Row 3 should equal the total in the Privacy Statistical Report Section 1.1 Row 5