

2014–2015 Annual Report to Parliament on the Administration of the *Privacy Act*



RC4415-1(E) Rev. 15



Canada Revenue
Agency

Agence du revenu
du Canada

Canada 



Foreword

Each fiscal year, the head of every government institution prepares and submits a report to Parliament on the administration of the *Privacy Act*.

This annual report is tabled in Parliament in accordance with section 72 of the *Privacy Act* under the direction of the Minister of National Revenue and the Commissioner of the Canada Revenue Agency (CRA). It describes how the CRA administered and fulfilled its obligations under the *Privacy Act* between April 1, 2014, and March 31, 2015. It also discusses emerging trends, program delivery, and areas of focus for the year ahead.

The *Privacy Act*

The *Privacy Act* came into force on July 1, 1983. It protects the privacy of individuals by outlining strong requirements for collecting, retaining, using, disclosing, and disposing of personal information held by government institutions. It provides individuals (or their authorized representatives) with a right of access to their own personal information, with limited and specific exceptions and with rights of correction or annotation or both. Individuals who are dissatisfied with any matter related to a formal request made under the *Privacy Act* are entitled to complain to the Privacy Commissioner of Canada.

The *Privacy Act*'s formal processes do not replace other means of obtaining government information. The CRA encourages individuals and their representatives to consider requesting information through the following informal methods:

- topical indexes on the CRA Web site: www.cra.gc.ca/azindex/menu-eng.html
- individual income tax enquiries (including requests for forms and publications): **1-800-959-8281**
- universal child care benefit, Canada child tax benefit and related provincial and territorial programs, child disability benefit, and children's special allowances enquiries: **1-800-387-1193**
- TTY (teletypewriter for persons who are deaf or hard of hearing or who have a speech impairment): **1-800-665-0354**



Table of Contents

Overview of the Canada Revenue Agency	4
Chief Privacy Officer	5
The Access to Information and Privacy Directorate	5
The Access to Information and Privacy Oversight Review Committee.....	6
Delegation of responsibilities under the <i>Privacy Act</i>	6
Schedule – <i>Privacy Act</i>	8
Statistical report (Appendix A) – Interpretation and explanation	9
Operational environment	12
Monitoring request inventories	15
Managing privacy breaches	15
Privacy impact assessments	17
Policies, guidelines, and procedures.....	20
Complaints, investigations, and Federal Court cases	20
Collaboration with oversight bodies and other organizations	21
Conclusion.....	27
Appendix A – Statistical report.....	28



Overview of the Canada Revenue Agency

The Canada Revenue Agency (CRA) administers tax laws for the Government of Canada and for most provinces and territories. It also administers various social and economic benefit and incentive programs delivered through the tax system. In addition, the CRA has the authority to enter into new partnerships with the provinces, territories, and other government bodies — at their request and on a cost-recovery basis — to administer non-harmonized taxes and other services. Overall, the CRA promotes compliance with Canada's tax legislation and regulations and plays an important role in the economic and social well-being of Canadians.

The Minister of National Revenue is accountable to Parliament for all of the CRA's activities, including administering and enforcing the *Income Tax Act* and the *Excise Tax Act*.

The *Canada Revenue Agency Act* provides for the establishment of a Board of Management consisting of 15 directors appointed by the Governor in Council. They include the Chair, the Commissioner and Chief Executive Officer, a director nominated by each province, one director nominated by the territories, and two directors nominated by the federal government. Under the provisions of the *Canada Revenue Agency Act*, the Board of Management oversees the organization and administration of the CRA, including the management of its resources, services, property, personnel, and contracts. In fulfilling this role, the Board of Management brings a forward-looking strategic perspective to the CRA's operations, fosters sound management practices, and is committed to efficient and effective service delivery.

As the CRA's chief executive officer, the Commissioner is responsible for the day-to-day administration and enforcement of the program legislation that falls under the Minister's delegated authority. The Commissioner is accountable to the Board of Management for managing the CRA, supervising employees, and implementing policies and budgets. Moreover, the Commissioner must assist and advise the Minister with respect to legislated authorities, duties, functions, and Cabinet responsibilities.

The CRA is made up of 12 branches and 5 regional offices across the country.

Branches

- Appeals
- Assessment and Benefit Services
- Audit, Evaluation, and Risk
- Compliance Programs
- Finance and Administration
- Human Resources
- Information Technology
- Legal Services
- Legislative Policy and Regulatory Affairs
- Public Affairs
- Strategy and Integration
- Taxpayer Services and Debt Management

Regions

- Atlantic
- Ontario
- Pacific
- Prairie
- Quebec



Chief Privacy Officer

The Assistant Commissioner, Public Affairs Branch, is the CRA's Chief Privacy Officer. The Chief Privacy Officer has a broad mandate for overseeing privacy at the CRA. To fulfill this mandate, the Chief Privacy Officer:

- oversees decisions related to privacy, including privacy impact assessments;
- champions personal privacy rights, including managing internal privacy breaches, according to legislation and policy; and
- reports to the CRA's senior management on the state of privacy management at the CRA at least twice a year.

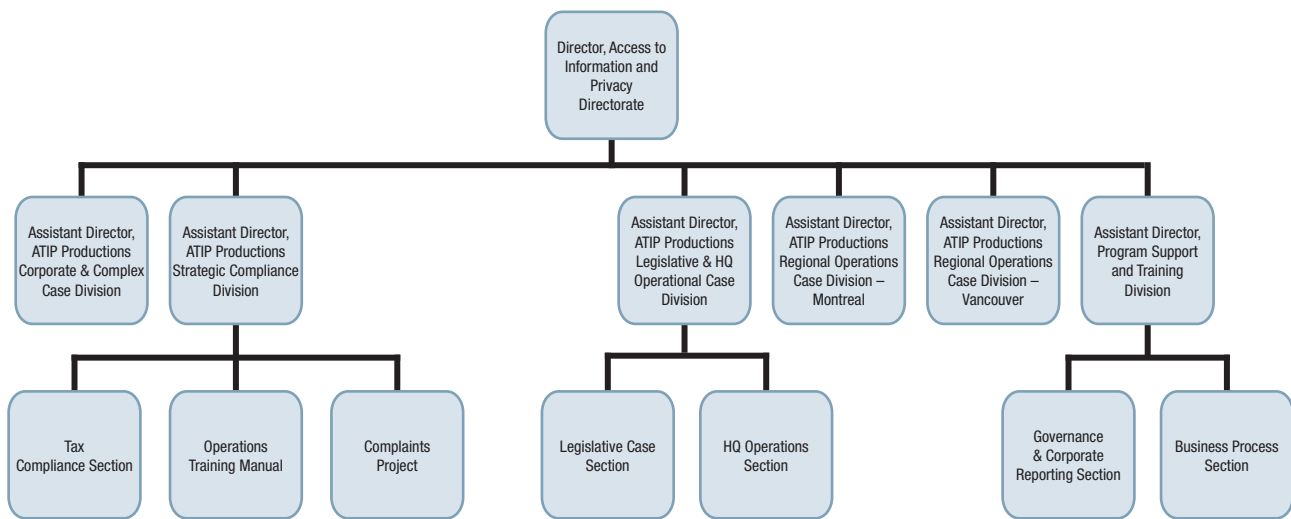
The Access to Information and Privacy Directorate

The Access to Information and Privacy (ATIP) Directorate helps the CRA meet its requirements under the *Access to Information Act* and the *Privacy Act*. To fulfill this mandate, the ATIP Directorate:

- responds to requests and enquiries under the *Access to Information Act* and the *Privacy Act*;
- provides advice and guidance to CRA employees on requests for, and the proper management and protection of, personal information under the CRA's control;
- coordinates privacy impact assessment processes within the CRA, including giving expert advice to CRA employees on privacy implications, risks, and options for avoiding or reducing risks;
- gives training and awareness sessions on the *Access to Information Act* and the *Privacy Act* and the practices and requirements for managing personal information;
- communicates with the Treasury Board Secretariat of Canada and the offices of the information and privacy commissioners of Canada about complaints, audits, and policy or legislative requirements; and
- fulfills corporate planning and reporting obligations such as the CRA's annual reports to Parliament on the administration of the *Access to Information Act* and the *Privacy Act*.

The Director of the ATIP Directorate has the full delegated authority of the Minister of National Revenue under the *Access to Information Act* and *Privacy Act*, manages and coordinates the ATIP program, leads strategic planning and development initiatives, and supports the Assistant Commissioner, Public Affairs Branch, and Chief Privacy Officer.

The ATIP Directorate is made up of two main divisions: process; and, program support and training (within the Directorate and CRA-wide). In addition to its headquarters office in Ottawa, the ATIP Directorate has an office in Vancouver and an office in Montréal. In 2014–2015, 117 full-time ATIP Directorate employees administered the *Access to Information Act* and the *Privacy Act*.



The Access to Information and Privacy Oversight Review Committee

The Access to Information and Privacy Oversight Review Committee is an assistant commissioner-level committee, chaired by the Chief Privacy Officer. The committee was established to ensure horizontal consultation, collaboration, and decision-making on emerging ATIP issues at the CRA. Among other responsibilities, the committee reviews high-risk privacy impact assessments, identifies measures to support more effective administration of ATIP-related matters, and champions ATIP-related activities.

Delegation of responsibilities under the *Privacy Act*

As head of the CRA, the Minister of National Revenue is responsible for how the CRA administers the *Privacy Act* and complies with the *Privacy Regulations* and Treasury Board Secretariat of Canada policy instruments. Section 73 of the *Privacy Act* gives the Minister of National Revenue the authority to designate one or more officers or employees of the CRA to exercise or perform all, or part, of the Minister's powers, duties, and functions under the Act.

The CRA's current delegation order for the *Privacy Act* was signed by the Minister of National Revenue on March 6, 2014. It identifies specific provisions of the *Privacy Act* and its regulations that the Minister has delegated to various positions within the CRA.

The Access to Information and Privacy Director and assistant directors, as well as the managers of the processing units, approve responses to requests under the *Privacy Act*. Delegations are also extended to the Commissioner, the Deputy Commissioner, and the Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch.



Minister
of National Revenue



Ministre
du Revenu national

Ottawa, Canada K1A 0A6

Privacy Act
Delegation Order

Arrêté sur la délégation en vertu de la *Loi sur la protection des renseignements personnels*

I, Kerry-Lynne D. Findlay, Minister of National Revenue, do hereby designate, pursuant to section 73 of the *Privacy Act*, the officers or employees of the Canada Revenue Agency who hold the positions set out in the attached Schedule to exercise or perform the powers, duties, or functions that have been given to me as head of a government institution under the provisions of the *Privacy Act* as set out in the Schedule.

This designation replaces all previous delegation orders.

Je, Kerry-Lynne D. Findlay, ministre du Revenu national, délègue par les présentes, en vertu de l'article 73 de la *Loi sur la protection des renseignements personnels*, aux cadres ou employés de l'Agence du revenu du Canada détenteurs des postes mentionnés dans l'annexe ci-jointe les attributions dont je suis, en qualité de responsable d'une institution fédérale, investie par les dispositions de la *Loi sur la protection des renseignements personnels* qui sont mentionnées dans l'annexe.

Le présent document remplace et annule tout arrêté antérieur.

La ministre du Revenu national,

Kerry-Lynne D. Findlay
Minister of National Revenue

Signed in Ottawa, Ontario, Canada this 6th day of March, 2014
Signé à Ottawa, Ontario, Canada le 6^e jour de mars 2014

Canada



Schedule – *Privacy Act*

The CRA positions authorized to perform the powers, duties, and functions given to the Minister of National Revenue as head of a government institution under the provisions of the *Privacy Act* and its regulations are the following:

Commissioner

- Full authority

Deputy Commissioner

- Full authority

Assistant Commissioner, Public Affairs Branch (PAB) and Chief Privacy Officer

- Full authority

Director, Access to Information and Privacy (ATIP) Directorate, PAB

- Full authority

Assistant directors, ATIP Directorate, PAB

- Full authority

Managers, ATIP Directorate, PAB

- Paragraphs 8(2)(j) and (m); subsections 8(5) and 9(1); sections 14 to 16; paragraphs 17(2)(b) and 17(3)(b), subsections 19(1) and 19(2); sections 20 to 22 and 23 to 28; subsections 33(2), 35(1) and 35(4) of the *Privacy Act*; and section 9 the *Privacy Regulations*.



Statistical report (Appendix A) – Interpretation and explanation

Appendix A provides a statistical report on the CRA’s activities under the *Privacy Act* for the 2014–2015 reporting period. The following explains and interprets the statistical information.

Requests under the *Privacy Act*

During this reporting period (April 1, 2014, to March 31, 2015), the CRA received 2,533 new privacy requests. This is an increase of 986 requests (64%) over last year’s total of 1,548 requests. With the 225 requests carried forward from 2013–2014, there were 2,758 active requests. Although there was a significant increase in the privacy requests received during the year compared with the previous year, the number of requests received in 2013–2014 was the third-lowest in the past ten years. The following table shows the number of privacy requests the CRA received and completed in the past five fiscal years.

Fiscal year	Requests received	Requests completed	Pages processed
2010–2011	2,600	2,767	725,741
2011–2012	1,362	1,497	510,503
2012–2013	1,980	1,936	775,563
2013–2014	1,548	1,553	624,430
2014–2015	2,533	2,313	636,207

Other Requests

In 2014–2015, the ATIP Directorate closed 14 consultation requests from other government institutions and organizations. A total of 730 pages were reviewed to respond to these requests. (For more details on the consultations received from other government institutions and organizations, including disposition and completion times, see Part 6 of Appendix A.)

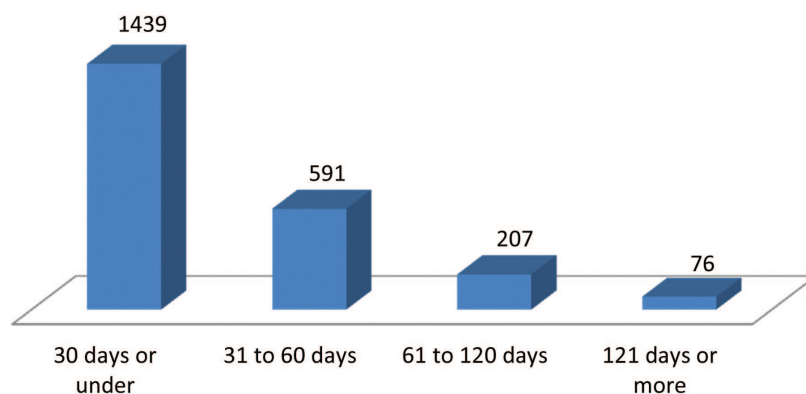
The ATIP Directorate’s Program Support and Training Division responded to 2,333 emails and 704 telephone enquiries from inside and outside the CRA. The responses included giving advice and guidance on processes and procedures related to the *Access to Information Act* and the *Privacy Act* and providing contact information.

Completion time and extensions

The following chart shows the completion times for the 2,313 requests closed in 2014–2015. Extensions were taken for 874 (38%) of these requests because meeting the original 30-day time limit would have interfered unreasonably with operations or because there was a need to consult others (for example, other individuals or other government departments).



Completion time



The ATIP Directorate completed 2,121 (91.7%) requests within the time frame required by law. This means that responses were provided within 30 calendar days or, if a time extension was taken, within the extended deadline.

Deemed refusals and complexities

A deemed refusal is a request that was closed after the deadline of 30 days set by law. Of the 2,313 requests closed during the reporting period, 192 were closed after the deadline, resulting in a deemed refusal rate of 8.3%.

Although the CRA continues to work toward a deemed refusal rate of zero, as the Office of the Privacy Commissioner recommended, the large volume of records that must be processed makes achieving this goal a continuing challenge.

The Treasury Board Secretariat developed criteria to determine if a request is complex. These criteria are: the number of pages to process; and the nature and sensitivity of the subject matter.

The CRA continues to handle a large number of requests that are considered complex based on the number of pages. For requests closed in 2014–2015, the CRA reviewed 636,207 pages. Of the 1,788 requests for which records were disclosed, 873 (49%) involved processing more than 100 pages, and 143 of these requests involved processing an average of 1,928 pages.

Other requests were considered complex because of the nature and sensitivity of the subject matter. (See table 2.5.3 of Appendix A for details.)



Dispositions of requests

During the reporting period, the ATIP Directorate completed 2,313 requests related to the *Privacy Act*.

- 729 were fully disclosed (31.52%)
- 1,059 were partially disclosed (45.78%)
- 6 were exempted in their entirety (0.26%)
- 0 were excluded in their entirety (0%)
- 49 resulted in no existing records (2.12%)
- 470 were abandoned by requesters (20.32%)
- 0 were neither confirmed nor denied (0%)

There was a notable increase in the requests abandoned this year (470) compared to last year (156). 262 of the abandoned requests were received online. 2014–2015 was the first year that requesters could submit a CRA *Privacy Act* request online. Of the 262 abandoned online requests, 110 were requests for a social insurance number; these requests were abandoned because they should have been sent to Service Canada and not the CRA. Analysis will continue in 2015–2016 to determine the reasons why such a high number of online requests were abandoned in 2014–2015.

For more details, see table 2.1 of Appendix A.

Exemptions

The *Privacy Act* allows an institution to sometimes refuse access to certain information. For example, information about individuals other than the requester cannot be disclosed if the individual has not given his or her consent. These types of refusals are called exemptions. They must be limited and relate to specific sections of the *Privacy Act*.

The CRA used the following sections of the Act to refuse access to information in full or in part for 1,065 (46%) of the 2,313 requests closed during the reporting period.

- Section 19 – personal information obtained in confidence (40 requests)
- Section 22 – law enforcement and investigation (467 requests)
- Section 22.3 – *Public Servants Disclosure Protection Act* (1 request)
- Section 25 – safety of individuals (1 request)
- Section 26 – information about another individual (912 requests)
- Section 27 – solicitor-client privilege (117 requests)

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.

There were no exclusions during the reporting period.



Format of information released

Requesters can choose to receive their response package in paper, CD, or DVD format. Providing documents electronically significantly reduces manual processes and paper consumption. In 2014–2015, of the 1,788 requests for which information was disclosed in full or in part, 1,308 requests (73%) were released in electronic format. This is a 17% increase over the previous reporting period. Of the 551,338 pages fully or partially disclosed in 2014–2015, 486,415 (88%) pages were released in electronic format.

Requests for translation

One request required the translation of records in 2014–2015.

Records are normally released in the language in which they exist; however, records may be translated in a particular official language when requested and where the institution considers a translation or interpretation to be necessary to help the requester understand the information.

Disclosures under paragraph 8(2)(m) of the *Privacy Act*

During the reporting period, there were no disclosures made under paragraph 8(2)(m) of the *Privacy Act*.

Paragraph 8(2)(m) provides that personal information may be disclosed for any purpose where, in the opinion of the head of an institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or disclosure would clearly benefit the individual to whom the information relates.

Corrections and notation

The CRA did not receive any requests to correct personal information in 2014–2015.

Costs

During 2014–2015, the ATIP Directorate's estimated total cost to administer the *Privacy Act* was \$4,329,167. This excludes significant support and resources from the branches and regions. For more details, see Appendix A.

Operational environment

As the chief administrator of federal, provincial, and territorial tax laws, the CRA maintains one of the Government of Canada's largest repositories of personal information, second only to Employment and Social Development Canada. In addition, the CRA collects and manages the personal information for its workforce of more than 40,000 individuals.



The trust Canadians place in the CRA to safeguard the privacy of their personal information is a cornerstone of the CRA's work. In 2014–2015, the CRA worked on many projects to enhance its privacy management framework.

Chief Privacy Officer Action Plan

The Chief Privacy Officer (CPO) oversees privacy management at the CRA. In 2013–2014, to support the CPO in achieving her mandate, the ATIP Directorate developed an action plan to make sure accountabilities, responsibilities, and activities related to privacy are reinforced and communicated across the CRA.

The action plan recognizes that all employees in all parts of the organization share the responsibility for managing privacy. The plan identifies key goals and assigns accountability for achieving them to specific areas within the CRA.

In 2014–2015, the ATIP Directorate worked with specific branches to set performance measures that can be used to monitor and report on progress against the goals and initiatives outlined in the action plan. The goals and initiatives are linked to requirements of the Treasury Board Secretariat, recommendations in the Privacy Commissioner's 2013 audit of the CRA's privacy management framework, and the action plans developed following the CRA's risk assessment in 2013 of unintentional privacy breaches.

These performance measures give the CPO a performance dashboard to continually assess and report twice yearly to senior management on the state of privacy management at the CRA.

ATIP action plan

As a result of a significant privacy breach within the ATIP Directorate in November 2014, the Directorate developed an action plan to enhance their privacy safeguards. See page 17 for more details.

Raising Awareness

To enhance employees' awareness of their privacy-related roles and responsibilities, the ATIP Directorate participated in two awareness events: Data Privacy Day and Security Awareness Week.

For the fourth consecutive year, the CRA joined the Office of the Privacy Commissioner and many other institutions across Canada and the world to promote Data Privacy Day. This initiative highlights the effect that technology has on privacy rights and underlines the importance of valuing and protecting personal information. The CRA's activities focused on the role all CRA employees play in safeguarding personal information in their day-to-day jobs. Over a week-long period, the ATIP Directorate highlighted these responsibilities across the CRA and promoted the many tools available to support employees in fulfilling them.

The ATIP Directorate also participated in the CRA's Security Awareness Week activities. Security Awareness Week was originally launched by the Treasury Board Secretariat and has become an



annual opportunity for government departments to discuss security topics, including those related to personal privacy (for example, identity theft).

As part of Security Awareness Week, the Finance and Administration Branch organized activities for employees, including an event at Library and Archives Canada. The ATIP Directorate set up an information kiosk on many privacy-related topics, such as privacy impact assessments, privacy breaches, and the role of the CPO at the CRA.

The ATIP Directorate also developed more targeted communications to help staff fulfil their ATIP-related responsibilities.

- **ATIP contacts:** These employees in the branches and regions respond to ATIP requests. They play a significant role in making sure the ATIP Directorate receives all the information it needs to process requests on time. In 2014–2015, the ATIP Directorate continued to support ATIP contacts by providing monthly emails and quarterly teleconference calls to share significant information with them and to let them seek clarification, and share challenges and solutions with their colleagues.
- **Project managers:** These employees need to be aware of their privacy-related obligations when it comes to designing and implementing projects. To help them do this, the ATIP Directorate updated the privacy practices toolkit to make sure project managers have the tools to manage privacy properly at all times.

Training

The ATIP Directorate provides training to CRA employees about the requirements of, and their responsibilities under, the *Access to Information Act* and the *Privacy Act*. This training is tailored to the needs of specific audiences. For instance, employees who have little or no knowledge of the subject take course ATIP 101. Subject matter experts take more specific training, such as on how to respond to requests for records.

In 2014–2015, ATIP training was given to 1,908 participants in 69 sessions across Canada. Also, 144 managers received online ATIP training under the CRA's management learning program. The ATIP Director also presented awareness sessions to two CRA senior management committees and gave several presentations at ATIP Oversight Review Committee meetings.

The CRA's Legal Services Branch also provided eight training sessions to 90 employees. These sessions focused on preparing documents for release in CRA reading rooms, on ATIP legal awareness, and on ATIP information for technology specialists.

Also during the fiscal year, all employees in the ATIP Directorate completed the mandatory CRA security awareness course.

Privacy projects

In 2014–2015, the ATIP Directorate continued to strengthen privacy management through two projects:

- privacy notices
- investigative bodies designation



Privacy notices

The *Privacy Act* requires that institutions use a privacy notice to tell individuals from whom they collect personal information why the information is being collected. The privacy notice must be inserted every time personal information is collected, whether it is on a paper or electronic form, an online application, or by any other method. Treasury Board Secretariat policies set out the content that the notices must contain.

In 2012–2013, the ATIP Directorate began reviewing CRA forms to make sure the CRA is following all legislative and Treasury Board policy requirements. Significant progress has been made and full privacy notices have been incorporated on the majority of the CRA's individual taxpayer returns and forms.

A working group has been set up to develop a plan for all other CRA forms that collect personal information, such as those that relate to corporations, GST, and benefit programs.

Investigative bodies designation

In 2013–2014, the ATIP Directorate continued to work with stakeholders to provide new and revised submissions to the Department of Justice Canada for investigative body designations under Schedules II and III of the *Privacy Regulations*. These schedules list investigative bodies of the federal government to which personal information can be disclosed for investigative purposes. Final submissions were provided to the Department of Justice Canada in 2014–2015. Once the investigative body submissions receive official approval from the Department of Justice, Schedule II of the *Privacy Regulations* will be updated.

Monitoring request inventories

The CRA's ATIP Directorate produces a monthly report that captures key statistical information about the CRA's inventory of ATIP requests. This report shows the average times for each of the key phases of request processing (for example, intake, search and locate records, and analysis). The report also provides statistical information about the number of extensions taken, completion times, pages processed, complaints, and complaint disposition.

The ATIP Director uses this report to monitor trends, measure ATIP Directorate performance, and determine any process changes required to improve performance. The inventory is a regular agenda item for senior management meetings within the ATIP Directorate.

Managing privacy breaches

The CRA has many controls in place to safeguard taxpayer information, including its Integrity Framework, information technology, and security controls. Despite these controls, privacy breaches sometimes occur. When they do, the CRA investigates and reports material breaches to the Office of the Privacy Commissioner and the Treasury Board Secretariat of Canada. Affected individuals are also notified if needed and measures are taken to prevent breaches from occurring again.



Effectively managing privacy breaches is a responsibility that the ATIP Directorate and the Security and Internal Affairs Directorate in the Finance and Administration Branch share through an information-sharing protocol.

Under the protocol, the Security and Internal Affairs Directorate must inform the ATIP Directorate of significant privacy breaches through its early notification process. It also must advise the ATIP Directorate that it is launching an investigation into an alleged privacy breach as a result of employee misconduct and within 30 days of the end of an investigation.

The Agency Security Officer decides whether affected individuals should be notified according to Treasury Board Secretariat requirements, and the ATIP Directorate must confirm that it agrees with this decision. When the ATIP Directorate disagrees with a decision about notifying affected individuals, the ATIP Director has to refer the case to the CPO for a final decision.

During 2014–2015, the CRA notified the Office of the Privacy Commissioner and the Treasury Board Secretariat of 37 material privacy breach incidents.

Privacy breaches involving taxpayer information generally fall into three broad categories: employee misconduct (such as unauthorized access, use, or disclosure of taxpayer information); unintentional breaches (such as human error, negligence, or procedural or mechanical issues); or breaches stemming from information technology vulnerabilities.

Of the 37 material privacy breach incidents reported to the Office of the Privacy Commissioner and the Treasury Board Secretariat in 2014–2015:

- 32 involved unauthorized access to taxpayer information by a CRA employee
- 2 involved unauthorized disclosure of taxpayer information
- 2 involved misdirected mail
- 1 stemmed from the theft of information

Two of these breaches generated significant public attention during the year: an incident involving the theft of information from the CRA's systems through the Heartbleed vulnerability and an incident involving the inadvertent release of personal information to the Canadian Broadcasting Corporation.

Integrity in the workplace is the cornerstone of the CRA's culture. The CRA supports its employees in doing the right thing by providing clear guidelines and tools to ensure privacy, security, and the protection of CRA programs and data. This includes:

- refreshing the Code of ethics and conduct;
- increasing integrity awareness through communications and tools;
- updating the CRA Integrity Framework annually;
- launching the anonymous internal fraud and misuse reporting line;
- modernizing the National Audit Trail System; and
- introducing the new Reliability + Personnel Security Screening.



Heartbleed vulnerability (theft of information)

In April 2014, there was a malicious breach of CRA's systems as a result of the Heartbleed vulnerability. The CRA quickly closed down e-services, including My Account and My Business Account, for five days to contain the vulnerability. While public confidence in the CRA's online services remained strong, an extensive lessons-learned exercise across government following the incident has resulted in new protocols for detecting and sharing information on information technology vulnerabilities.

Inadvertent release of information to the Canadian Broadcasting Corporation (misdirected mail)

In November 2014, a CRA employee inadvertently sent the wrong package of information to an access to information requester who was a Canadian Broadcasting Corporation (CBC) journalist. An investigation confirmed that taxpayer information had been disclosed as a result of human error. In spite of the CRA's efforts to retrieve the information, the CBC chose to publish some of the information in an article.

The CRA immediately addressed the incident by conducting an internal investigation and implementing a plan to enhance controls within the CRA's ATIP operations. The plan's enhancements focus on three broad areas: operational processes, communications and training, and accountabilities.

Many of these activities have already been implemented, including the following:

- completion of role-specific training and mandatory security training by all ATIP Directorate staff;
- introduction of additional quality assurance measures at the mail-out stage of the process for preparing and sending request responses; and
- additional tracking system gates to reinforce critical steps in processing a request.

The CRA also initiated a third-party independent review of its access to information and privacy management frameworks. The recommendations from that review will be implemented in 2015–2016.

Privacy impact assessments

In its 2013 audit of the CRA's privacy management framework, the Office of the Privacy Commissioner recommended that the CRA complete and approve privacy impact assessments (PIAs) before implementing any new program or initiative that might cause privacy risks to taxpayer information. In response, the CRA created a risk-based PIA plan that aligns with its program activity architecture. The plan, which is renewed and updated periodically, includes 40 PIAs. New PIAs will be added to the plan as required.

During the reporting period, the CRA completed six PIAs and sent them to the OPC and the Treasury Board Secretariat for review. An additional 88 initiatives were reviewed to assess potential privacy concerns. This involved reviewing documents such as privacy assessment determination questionnaires, threat and risk assessments, and memorandums of understanding.



The ATIP Directorate also contracted PIA specialists to help program areas complete their PIAs, and has adopted a portfolio approach to support program branches.

In line with the Treasury Board Secretariat's Directive on Privacy Impact Assessment, the CRA releases summaries of completed PIAs on its website (www.cra.gc.ca/gncy/prvcy/pia-efvp/menu-eng.html). The following are the summaries of the six PIAs completed in 2014–2015:

GST/HST Returns and Rebates Processing Program

This PIA covers the workload within the Business Returns Directorate for GST/HST tax returns, rebate applications and various elections that are filed by businesses, third parties and individuals. It pertains to the GST/HST that businesses and third parties collect and submit and to GST/HST that individuals and businesses pay where a rebate applies. It also covers various elections that businesses can make to amend certain aspects of their GST/HST account, for example, changing a filing frequency. This PIA does not include the GST/HST credit program, which is available to individuals based on income thresholds and is issued every three months. This program is administered by the Benefit Programs Directorate.

Recent changes to the program include:

1. Administering the Prince Edward Island harmonized sales tax. As with several other provinces, PEI reached an agreement with the Government of Canada to harmonize its provincial sales tax with the GST effective April 1, 2013. The CRA administers all aspects of the PEI HST, including processing HST returns, rebates, and elections.
2. Administering the GST and the Quebec Sales Tax (QST) for selected listed financial institutions that have a permanent establishment in Quebec and those that have a permanent establishment outside Quebec but do business in Quebec.
3. Effective April 13, 2015, collecting and storing the Internet protocol address used to file an electronic GST/HST return.

Scientific Research and Experimental Development (SR&ED) Incentive Program (Enhanced Expenditures Claim, Form T661)

Budget 2013 introduced measures to give the CRA administrative tools to improve risk assessment. Form T661, the SR&ED expenditures claim form, was revised to ask for more detailed information about claim preparers and billing arrangements. In particular, if one or more third parties helped to prepare a claim, the business number of each third party now has to be included. The form also asks for details about the billing arrangements, including whether contingency fees were used and the amount of the fees payable. If no third party was involved, the claimant now has to certify that no third party helped in any way to prepare the SR&ED claims. The CRA will carefully analyze the additional information required to see if there is any correlation with a higher risk of non-compliance in SR&ED claims.



Telephone Enquiries Program

The CRA's telephone enquiries program provides support to individuals, benefit recipients, businesses, and trusts. It helps them meet their tax obligations, make them aware of their benefit entitlements, and helps them with their general or account-specific enquiries. The program encourages compliance because callers can address any issues or get information they need to meet their obligations and receive their benefit entitlements.

The telephone enquiries program introduced the Email Link Management System, which allows call centre agents to send an email to a taxpayer that contains a link to a form or publication.

Authentication and Credential Management Services

The CRA has been a major stakeholder in the Government of Canada Cyber-Authentication Renewal Initiative. As part of the initiative, the CRA provides its own authentication and credential management service for individuals, business owners, and representatives to use when they access the CRA's online services.

T1 Residency Project

The CRA administers tax, credits, and benefit programs on behalf of certain provinces and territories to provide better service to taxpayers. The province of Newfoundland and Labrador has expressed growing concern with the residency status of some Canadian taxpayers who file their return as residents of one province but get their services from another province. The tax collection agreements commit the CRA to making a reasonable effort to counter false claims of residency.

The CRA is establishing a new arrangement whereby Newfoundland and Labrador would give the CRA more information, in order to allow the CRA to more effectively use its financial resources on cases where the risk of non-compliance is higher.

International Electronic Funds Transfers Business Intelligence

Economic Action Plan 2013 highlighted that international tax evasion and aggressive tax avoidance cost governments and taxpayers worldwide and are unfair to the businesses and individuals who do play by the rules. It introduced measures to address international tax evasion and aggressive tax avoidance.

These measures included a requirement for some financial intermediaries to report international electronic funds transfers of \$10,000 or more to the CRA. The main objective is to generate intelligence and leads that are relevant to tax non-compliance, particularly offshore tax non-compliance. Financial institutions began reporting on January 1, 2015. Reporting entities must provide information on the person conducting the transaction, the recipient of the funds, the transaction itself, and the financial intermediaries facilitating the transaction.



Policies, guidelines, and procedures

Procedures on the disclosure of personal information under subsection 8(2) of the *Privacy Act*

Subsection 8(2) of the *Privacy Act* outlines circumstances where personal information can be disclosed. In 2014–2015, after extensive consultations, the CRA finalized procedures on disclosing personal information. They will be formally approved in 2015–2016.

The procedures will ensure consistency and accountability in how personal information is disclosed across the CRA. They will help CRA employees and managers determine when disclosure under the *Privacy Act* is warranted, based on limited and specific criteria, and who should approve the disclosures.

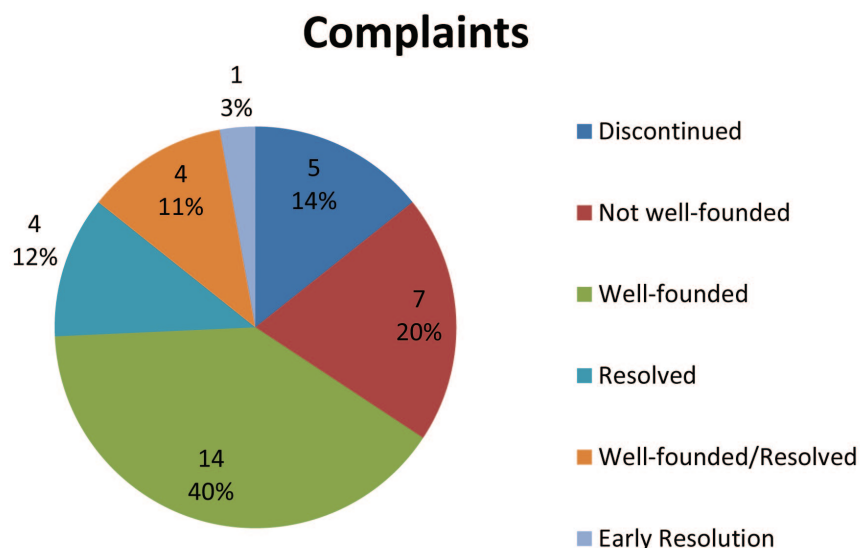
CRA privacy policy suite

In its 2013 audit of the CRA's privacy management framework, the Office of the Privacy Commissioner recommended that the CRA define fully the role of the CPO and monitor how the CPO's mandate is implemented in terms of awareness of employee privacy, reduction of privacy risk, and overall CRA compliance with the *Privacy Act*. The CRA privacy policy suite was revised to clarify the CPO role. These changes will be formally approved and communicated to employees in 2015–2016.

Complaints, investigations, and Federal Court cases

During 2014–2015, the CRA received 31 complaints under the *Privacy Act* and closed 35 complaints. The following chart details the disposition of the complaints closed during the fiscal year. (For definitions of the disposition categories, go to www.priv.gc.ca/cf-dc/def2_e.asp.)

One case went to Federal Court.





There were no complaints with a disposition of “settled during the course of investigation” during the reporting period.

The ATIP Directorate also received 164 complaints about alleged improper access, collection, use, or disclosure of personal information by the CRA. Complaints came from a variety of areas including the Office of the Privacy Commissioner, individuals, and the CRA’s Security and Internal Affairs Directorate.

Outstanding from previous fiscal year	Received during fiscal year	Completed	Closing inventory
51	164	137	78

Effectively managing privacy breaches is critical in maintaining public confidence in the integrity of the CRA. The CRA takes all breaches very seriously and is strengthening its controls and sanctions for unauthorized access and disclosure. (See “Privacy breach management” for details.)

Collaboration with oversight bodies and other organizations

The CRA continues to work closely with the Office of the Privacy Commissioner, the Treasury Board Secretariat of Canada, and other organizations to strengthen privacy management at the CRA.

Office of the Privacy Commissioner audit

In 2012–2013, the Office of the Privacy Commissioner completed an audit of the CRA’s privacy management framework as a follow-up to its February 2009 audit, “Privacy Management Frameworks of Selected Federal Institutions.” The CRA is on track to complete six of the nine audit recommendations in 2015–2016. Other activities will be fully implemented by 2016–2017 because they require the development and deployment of new Agency-wide IT systems and controls.



Recommendation	CRA progress
<p>The Canada Revenue Agency should define fully the role of the Chief Privacy Officer and monitor the implementation of the position's mandate in terms of employee privacy awareness, privacy risk reduction and overall Agency compliance with the <i>Privacy Act</i></p>	<ul style="list-style-type: none"> ■ Established performance measures to monitor and report on progress against the goals and initiatives outlined in the CPO action plan. ■ Drafted internal communications policy to promote the mandate of the CPO. ■ The CPO presented an update on the state of privacy at the CRA to senior management at least twice during the fiscal year. <p>This recommendation was fully implemented in 2014–2015.</p>
<p>Consistent with the Treasury Board Directive on Privacy Impact Assessments, the CRA should complete, review and approve privacy impact assessments prior to the implementation of any new program or initiative that may raise privacy risks to taxpayer information; and ensure that its ATIP Directorate is notified of all breaches as they are discovered.</p>	<ul style="list-style-type: none"> ■ Implemented a CRA-wide PIA plan. The plan is continually updated. At the end of the fiscal year, there were 40 PIAs in the plan. <p>Full implementation in 2015–2016.</p>
<p>The Canada Revenue Agency should implement a Certification and Accreditation process that clearly assigns accountability and responsibility for the management of the process, as well as oversight to ensure CRA documentation is approve on time.</p> <p>The Canada revenue Agency should also prioritize critical systems and all related applications to ensure they undergo the Certification and Accreditation process and Treat and Risk Assessments.</p>	<ul style="list-style-type: none"> ■ Launched a revised security assessment and authorization process for future enterprise applications. ■ Continued to conduct annual status updates for all security evaluations completed since 2008. ■ Continued to address missing threat and risk assessments for high-priority applications. ■ Ensured local application repository Web application is in place so that proper security evaluations are completed and tracked. <p>Full implementation in 2015–2016.</p>



Recommendation	CRA progress
<p>The Canada Revenue Agency should:</p> <ul style="list-style-type: none"> ■ ensure that its policies, practices and procedures are followed to manage local applications and adequate safeguards are used to protect the taxpayer information they contain; ■ ensure that its Local Application Repository is reviewed regularly for completeness, accuracy and currency; and ■ follow-up at each stage of the review and quality assurance processes and ensure that all local applications are approved by delegated officials before implementation. 	<ul style="list-style-type: none"> ■ Conducted a review of the existing procedures and safeguards, together with a current-state assessment of the local application repository. ■ Developed an action plan to close gaps in the local application repository. ■ Enhanced the governance process to include a mandatory review and approval process focusing on confirmation that PIAs and technical security reviews are completed before they are deployed to make sure they are complete, accurate, and current. <p>This recommendation was fully implemented in 2013–2014.</p>
<p>The Canada Revenue Agency should continue to enhance its Identity and Access Management System controls to ensure that employee access is limited to only that information required to carry out their job functions, based on the need-to-know principle.</p>	<ul style="list-style-type: none"> ■ Ongoing review of the roles and profiles managers use to provide accesses for their employees with the highest-priority applications. ■ Continued to implement an enhanced annual verification process of the CRA systems' access roles and profiles. ■ Continued to implement the identity and access management program: <ul style="list-style-type: none"> ■ Phase 3 (password management) (implementation planned for March 2016). ■ Phase 4 (access management) (implementation planned for March 2017). <p>Full implementation in 2016–2017.</p>



Recommendation	CRA progress
<p>The Canada Revenue Agency should review existing generic user IDs, ones shared by several individuals working on the same project or activity, to determine whether they are required, authorized and controlled; and should delete all IDs that are not in use.</p> <p>The Canada Revenue Agency should also ensure that all generic user IDs are subject to established review and approval processes.</p> <p>Consistent with Treasury Board Guidelines for Privacy Breaches, the Canada Revenue Agency should ensure that the Access to Information and Privacy Directorate is notified of all breaches as they are discovered.</p>	<ul style="list-style-type: none"> ■ Enhanced controls to reduce the number of generic accounts. ■ Continued to leverage the authoritative identity store implemented in May 2013 to review existing generic accounts, delete those not in use, and assign accountability for each account to designated individuals. ■ Continued to enhance security awareness and accountability for generic accounts. <p>Full implementation in 2015–2016.</p>
<p>The Canada Revenue Agency should continue to strengthen its audit logging system and process and the Agency should incorporate risk assessment tools to flag potentially inappropriate employee activities on its systems.</p>	<ul style="list-style-type: none"> ■ Implemented the new audit trail record analysis tool to help management review employee accesses. ■ Continued to enhance technological tools and associated business processes to analyze user transactions and identify issues and questionable patterns. ■ Awarded the contract for the Enterprise Fraud Management System. Testing of the system continues and implementation is planned for March 2017. <p>Full implementation in 2016–2017.</p>
<p>The Canada Revenue Agency should ensure adequate measures are in place to mitigate the risks associated with developer access to taxpayer information in test environments.</p> <p>The Canada Revenue Agency should also rigorously control, track and monitor transfers of taxpayer information from operational to test environments.</p>	<ul style="list-style-type: none"> ■ Updated and communicated the policy suite concerning populating and accessing taxpayer data in test environments. ■ Developed an options analysis to identify the most effective method to control, track, and monitor transfers of taxpayer information from operational to test environments. <p>Full implementation in 2016–2017.</p>



Recommendation	CRA progress
<p>Consistent with Treasury Board Guidelines for Privacy Breaches, the Canada Revenue Agency should ensure that the Access to Information and Privacy Directorate is notified of all breaches as they are discovered.</p>	<ul style="list-style-type: none"> ■ The Security and Internal Affairs Branch ensures that the ATIP Directorate is notified of all breaches as they are discovered. ■ Reviewed information-sharing protocol between Security and Internal Affairs Directorate and the ATIP Directorate to ensure consistency with Treasury Board guidelines for privacy breaches. ■ Reviewed and revised existing corporate policy instruments and responsibilities to reflect the appointment of the Chief Privacy Officer. Security and Internal Affairs Directorate’s corporate policy instruments approved, CRA privacy policy instruments scheduled to be approved in 2015–2016. <p>Full implementation in 2015–2016.</p>

Treasury Board Secretariat of Canada

The CRA consulted with the Treasury Board Secretariat’s Information and Privacy Policy Division on numerous occasions. CRA officials also participated in ATIP community meetings that the Treasury Board led throughout the fiscal year. The CRA’s ATIP Coordinator participated in three panel discussions during these meetings.

The CRA also participated in the Treasury Board Secretariat’s director general-level ATIP Training Working Group. The group established six priorities for 2014–2015 to modernize ATIP training in the Government of Canada:

- privacy basics, including PIAs
- preventing, managing, and reporting privacy breaches
- ATIP awareness training for the executive cadre in government
- Cabinet confidences and the revised consultation process
- most-frequently invoked exemptions
- ATIP general awareness

Several ATIP Directorate employees participated on the sub-working groups to develop training products for these six priorities.



In April 2014, the CRA joined the ATIP “request and pay online” initiative. This initiative has significantly decreased the number of ATIP requests received by mail. The CRA is also a member of the Request and pay online design working group. The CRA provides ongoing feedback to the group on the online request initiative to improve its functionality. The CRA also tracks the number of online requests received compared to the total number of requests received from all other methods to assess whether the public is receptive to this new method of access.

House Standing Committee on Access to Information, Privacy and Ethics

In April 2014, three senior CRA officials, including the Chief Privacy Officer, appeared before the House Standing Committee on Access to Information, Privacy and Ethics. The CRA was one of several institutions invited to appear before the Committee to support its study on the growing problem and impact of identity theft.



Conclusion

The CRA takes privacy and the safeguarding of personal information very seriously. In 2015–2016, the CRA will continue to strengthen its operations and privacy governance by:

- delivering targeted communications and training to key internal and external audiences with an emphasis on informal and proactive disclosure and privacy management
- monitoring and evaluating performance to address ATIP challenges promptly
- increasing quality assurance and process improvements
- implementing the Chief Privacy Officer Action Plan to make sure privacy accountabilities, responsibilities, and activities are formalized and communicated



Appendix A – Statistical report

Statistical Report on the *Privacy Act*

Name of institution: Canada Revenue Agency

Reporting period: April 1, 2014 to March 31, 2015

PART 1 – Requests under the *Privacy Act*

Number of requests

	Number of requests
Received during reporting period	2,533
Outstanding from previous reporting period	225
Total	2,758
Closed during reporting period	2,313
Carried over to next reporting period	445

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	131	453	127	12	3	1	2	729
Disclosed in part	26	331	447	189	26	25	15	1059
All exempted	1	1	2	1	1	0	0	6
All excluded	0	0	0	0	0	0	0	0
No records exist	11	29	5	1	0	3	0	49
Request abandoned	415	41	10	4	0	0	0	470
Neither confirmed nor denied	0	0	0	0	0	0	0	0
Total	584	855	591	207	30	29	17	2,313



2.2 Exemptions

Section	Number of requests	Section	Number of requests	Section	Number of requests
18(2)	0	22(1)(a)(i)	10	23(a)	0
19(1)(a)	7	22(1)(a)(ii)	27	23(b)	0
19(1)(b)	0	22(1)(a)(iii)	1	24(a)	0
19(1)(c)	30	22(1)(b)	427	24(b)	0
19(1)(d)	3	22(1)(c)	1	25	1
19(1)(e)	0	22(2)	0	26	912
19(1)(f)	0	22.1	1	27	117
20	0	22.2	0	28	0
21	0	22.3	1		

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	282	447	0
Disclosed in part	198	861	0
Total	480	1,308	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	42,482	42,477	729
Disclosed in part	572,800	508,861	1,059
All exempted	6,978	0	6
All excluded	0	0	0
Request abandoned	13,947	13,619	470
Neither confirmed nor denied	0	0	0
Total	636,207	564,957	2,264

2.5.2 Relevant pages processed and disclosed by size of requests

Disposition of requests	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	614	18,743	112	19,894	1	797	2	3,043	0	0
Disclosed in part	301	14,925	466	116,868	151	104,398	138	255,517	3	17,153
All exempted	6	0	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0	0	0
Request abandoned	465	47	0	0	3	2,140	1	2,165	1	9,267
Neither confirmed nor denied	0	0	0	0	0	0	0	0	0	0
Total	1,386	33,715	578	136,762	155	107,335	141	260,725	4	26,420



2.5.3 Other complexities

Disposition	Consultation required	Legal advice sought	Interwoven information	Other	Total
All disclosed	1	3	0	3	7
Disclosed in part	14	3	1	11	29
All exempted	1	0	0	1	2
All excluded	0	0	0	0	0
Request abandoned	0	2	4	15	21
Neither confirmed nor denied	0	0	0	0	0
Total	16	8	5	30	59

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
192	156	2	4	30

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	14	40	54
16 to 30 days	0	18	18
31 to 60 days	8	32	40
61 to 120 days	5	24	29
121 to 180 days	5	11	16
181 to 365 days	8	14	22
More than 365 days	0	13	13
Total	40	152	192



2.7 Requests for translation

Translation Requests	Accepted	Refused	Total
English to French	1	0	1
French to English	0	0	0
Total	1	0	1

Part 3 – Disclosures under subsection 8(2) and 8(5)

Disclosures under subsection 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

Requests for correction of personal information and notations

Disposition for correction requests received	Number
Notations attached	0
Requests for correction accepted 0	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 Section 70	15(a)(ii) Consultation Other	15(b) Translation or conversion
All disclosed	123	0	0	0
Disclosed in part	645	0	4	0
All exempted	3	0	0	0
All excluded	0	0	0	0
No records exist	4	0	0	0
Request abandoned	10	0	0	0
Total	785	0	4	0



5.2 Length of extensions

Length of extensions	15(a)(i) Interference with operations	15(a)(ii) Consultation Section 70	15(a)(ii) Consultation Other	15(b) Translation purposes
1 to 15 days	8	0	0	0
16 to 30 days	777	0	4	0
Total	785	0	4	0

Part 6 – Consultations received from other institutions and organizations

6.1 Consultations received from other government institutions and organizations

Consultations	Other government of Canada institutions	Number of pages to review	Other organizations	Number of pages to review
Received during the reporting period	10	697	4	33
Outstanding from the previous reporting period	0	0	0	0
Total	10	697	4	33
Closed during the reporting period	10	697	4	33
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	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	4	0	1	0	0	0	0	5
Disclosed in part	4	0	0	1	0	0	0	5
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	8	0	1	1	0	0	0	10

6.3 Recommendations and completion time for consultations received from other organizations

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	1	1	0	0	0	0	0	2
Disclosed in part	1	1	0	0	0	0	0	2
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	2	2	0	0	0	0	0	4



Part 7 – Completion time of consultations on Cabinet confidences

7.1 Requests with Legal Services

Number of Days	Fewer Than 100 Pages Processed		101-500 Pages Processed		501-1000 Pages Processed		1001-5000 pages processed		More than 5000 pages processed	
	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed
1 to 15	0	0	0	0	0	0	0	0	0	0
16 to 30	0	0	0	0	0	0	0	0	0	0
31 to 60	0	0	0	0	0	0	0	0	0	0
61 to 120	0	0	0	0	0	0	0	0	0	0
121 to 180	0	0	0	0	0	0	0	0	0	0
181 to 365	0	0	0	0	0	0	0	0	0	0
More than 365	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0

7.2 Requests with Privy Council Office

Number of Days	Fewer Than 100 Pages Processed		101-500 Pages Processed		501-1000 Pages Processed		1001-5000 pages processed		More than 5000 pages processed	
	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed	Number of requests	Pages disclosed
1 to 15	0	0	0	0	0	0	0	0	0	0
16 to 30	0	0	0	0	0	0	0	0	0	0
31 to 60	0	0	0	0	0	0	0	0	0	0
61 to 120	0	0	0	0	0	0	0	0	0	0
121 to 180	0	0	0	0	0	0	0	0	0	0
181 to 365	0	0	0	0	0	0	0	0	0	0
More than 365	0	0	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0



Part 8 – Complaints and investigations notices received

Section 31	Section 33	Section 35	Court action	Total
31	0	35	1	67

Part 9 – Privacy impact assessments (PIAs)

Number of PIAs completed	6
--------------------------	---

Part 10 – Resources related to the *Privacy Act*

10.1 Costs

Expenditures		Amount \$
Salaries		\$3,680,087
Overtime		\$45,201
Goods and Services		\$603,879
– Professional services contracts	\$462,897	
– Other	\$140,982	
Total		\$4,329,167

10.2 Human Resources

Resources	Person years dedicated to privacy activities
Full-time employees	54.00
Part-time and casual employees	0.00
Regional staff	0.00
Consultants and agency personnel	2.50
Students	1.00
Total	57.50