



Now and Tomorrow  
Excellence in Everything We Do

# Annual Report on the Administration of the *Privacy Act*

Human Resources and Skills Development Canada  
2012–2013

You can download this publication by going online: <http://www12.hrsdc.gc.ca>

This document is available on demand in multiple formats (large print, Braille, audio cassette, audio CD, e-text diskette, e-text CD, or DAISY), by contacting 1 800 O-Canada (1-800-622-6232). If you use a teletypewriter (TTY), call 1-800-926-9105.

© Her Majesty the Queen in Right of Canada, 2013

For information regarding reproduction rights, please contact Public Works and Government Services Canada at: 613-996-6886 or [copyright.droitdauteur@pwgsc-tpsgc.gc.ca](mailto:copyright.droitdauteur@pwgsc-tpsgc.gc.ca)

**PDF**

Cat. No.: HS1-13-2-2013E-PDF

ISSN: 978-1-100-17322-1

**HRSDC**

Cat. No.: CA-600-06-13E

## **Table of Contents**

Executive Summary.....	4
Introduction .....	6
Privacy Management at HRSDC.....	8
HRSDC’s Legal Framework for Privacy .....	8
HRSDC’s Privacy Delegations.....	8
HRSDC’s Policy Framework for Integrated Privacy Management .....	9
Privacy Governance at HRSDC.....	9
Organization of the Privacy Function at HRSDC.....	11
Privacy Activities and Accomplishments for 2012–2013.....	13
Action Plan on the Minister’s Commitment to Information Security.....	13
2012–2013 Privacy Renewal Action Plan .....	14
Info Source Pilot Project.....	16
Privacy Performance Reporting for 2012–2013 .....	18
Requests for Information under the <i>Privacy Act</i> .....	18
Completed Privacy Impact Assessments.....	22
Privacy Training and Awareness Activities.....	24
Public Interest Disclosures .....	25
Complaints and Investigations .....	26
Moving Forward in 2013–2014.....	27
Annex A: Delegation Order .....	28
Annex B: Statistical Report on the <i>Privacy Act</i> .....	49

## **Executive Summary**

The effective management and protection of personal information is fundamental to the delivery of the Human Resources and Skills Development Canada (HRSDC) mandate. As one of the largest and most regionally present departments in the Government of Canada, HRSDC is responsible for the day-to-day management of more than 70 programs delivered directly to Canadians. In 2011–2012, a total of 140.5 million payments for Employment Insurance (EI), the Canadian Pension Plan (CPP) and Old Age Security (OAS) were paid to Canadians, representing \$90.6 billion in benefits. HRSDC interacts daily with Canadian citizens through Service Canada’s national multi-channel network. In 2011–2012, Service Canada provided service to 9 million visitors at more than 600 points of service, 65 million callers to its call centre network and some 77 million visitors to [servicecanada.gc.ca](http://servicecanada.gc.ca).

The delivery of many of the Department’s programs requires that Canadians provide their personal information to receive the benefits and services for which they are eligible. Each day the Department collects, uses and manages more personal information than any other federal government organization—personal information which is critical to the development and delivery of programs and services. In support of its programs and services for Canadians, the Department also shares personal information with its partners, including other federal departments and other levels of government.

The management and sharing of personal information is subject to a complex legal framework consisting of the *Privacy Act* as well as a specific “Privacy Code” that is contained within Part IV of the *Department of Human Resources and Skills Development Act* (DHRSD Act). The Department’s Privacy Code imposes standards for the management and protection of personal information that exceed the requirements of the *Privacy Act*. The Privacy Code reinforces the importance of personal information protection as an organizational value and recognizes that privacy protection is a necessary pre-condition to maintaining the public’s trust.

Important progress was made in advancing the Department’s privacy renewal agenda in fiscal year 2012–2013. Program-led Privacy Action Plans were developed for HRSDC’s major statutory programs and are being implemented across the organization. Departmental privacy policies and processes were also modernized, including the streamlining of the Privacy Impact Assessment process and the implementation of a new Directive on How to Respond to Security Incidents Involving Personal Information. Work was also initiated to formalize the privacy roles and responsibilities of all employees and to finalize a new Departmental Policy on Privacy Management. Other important priorities advanced in 2012–2013 include focussed attention on privacy awareness activities and the development of mandatory online privacy training for all employees.

In 2012–2013, pursuant to the 2012 *Budget Implementation Act*, the Department also harmonized and consolidated privacy provisions contained in five pieces of departmental and program legislation into a single Privacy Code under the DHRSD Act. On March 1, 2013, the regulations finalizing the implementation of the Privacy Code were completed and brought into force.

Despite these achievements, the privacy incidents in 2012–2013 involving the loss of personal information by the Department altered the trajectory of privacy renewal priorities at HRSDC. Statements from the Honourable Diane Finley, Minister of Human Resources and Skills Development, and the response from the Department underscored the seriousness of these events and HRSDC's commitment to take action.

These events highlighted the important role that each and every employee plays in the day-to-day management of personal information, the responsibility of all employees to protect the sensitive and personal information under their control and the importance of deepening efforts to foster an organizational culture rooted in the stewardship of departmental information assets. Moreover, the incidents have focused attention in the near term on the importance of an integrated approach to effective privacy protection, which includes robust information management practices, appropriate security safeguards and mandatory training. Over the longer term, the Department will continue its efforts to promote a proactive, risk-based approach to privacy management and nurture an organizational culture committed to the stewardship of personal information.

## **Introduction**

The *Privacy Act*, which came into force on July 1, 1983, imposes obligations on federal government departments and agencies to respect the privacy rights of individuals by limiting the collection, use and disclosure of personal information. The Act also gives individuals the right of access to their personal information and the right to request the correction of that information. Section 72 of the *Privacy Act* requires the head of each federal institution subject to the Act to submit an annual report to Parliament on the administration of the Act following the close of each fiscal year.

This report describes how Human Resources and Skills Development Canada (HRSDC) fulfilled its *Privacy Act* responsibilities during fiscal year 2012–2013.

HRSDC's mission is to build a stronger and more competitive Canada, to support Canadians in making choices that help them live productive and rewarding lives and to improve Canadians' quality of life. The Department delivers a range of programs and services that affect Canadians throughout their lives through three business lines: programs that support human resources and skills development, the Labour Program and Service Canada.

To fulfill its mission, the Department is responsible for:

- supporting a flexible national labour market;
- increasing participation in the labour force;
- removing barriers to post-secondary education attainment and skills development;
- overseeing federal labour responsibilities;
- providing income support to seniors, the disabled, families with children and Employment Insurance beneficiaries; and
- delivering certain Government of Canada programs and services on behalf of other departments and agencies.

Included in these core roles are responsibilities for the design and delivery of some of the Government of Canada's most well-known statutory programs and services, including:

- Old Age Security;
- the Canada Pension Plan;
- Employment Insurance;
- Canada Student Loans and Grants;
- the Canada Education Savings Program;
- the National Child Benefit; and
- the Universal Child Care Benefit.

These direct benefits to Canadians are part of Canada's social safety net and represent almost 95% of the Department's expenditures.

## **Privacy Management at HRSDC**

HRSDC is one of the largest and most regionally present federal departments in the Government of Canada. Citizens and clients interact with HRSDC on a daily basis through hundreds of points of service. The Department works in collaboration with partners and stakeholders in the not-for-profit sector, the private sector and other levels of government within Canada and beyond. HRSDC maintains an inventory of approximately 500 formal agreements for the exchange of personal information that have been established to facilitate work with partners and enable the efficient and effective delivery of services to clients.

The management of the Department's personal information holdings is a complex undertaking. Client personal information is located both physically and electronically across several systems, program areas, branches, offices and regions across the country. For many programs, responsibility for the protection of personal information throughout the program life cycle is shared across branches and regions. In addition, HRSDC is broadly recognized as holding more personal information than any other department in the Government of Canada.

### **HRSDC's Legal Framework for Privacy**

The *Privacy Act* protects the privacy of individuals with respect to personal information about themselves held by a government institution, and it provides individuals with a right of access to that information as well as a right to request correction of inaccurate information. Sections 4 to 8 of the *Privacy Act*, commonly referred to as the Code of Fair Information Practices, govern the collection, use, disclosure, retention and disposal of personal information.

In addition to the *Privacy Act*, HRSDC's management of personal information is governed by Part 4 of the *Department of Human Resources and Skills Development Act* (DHRSD Act), also referred to as the Privacy Code, which establishes the rules that apply to the protection, use and making available of personal information obtained and prepared by HRSDC. The Privacy Code contains provisions which go beyond subsection 8(2) of the *Privacy Act* in governing HRSDC's protection and disclosure of personal information.

### **HRSDC's Privacy Delegations**

Section 73 of the *Privacy Act* and section 11 of the DHRSD Act empower the head of the institution to delegate any of the powers, duties or functions assigned to him or her by those Acts to employees of the institution. In August 2010, Minister Finley approved a Delegation Order for the *Privacy Act*, DHRSD Act and *Department of Social Development Act* (repealed), which is attached as Annex A.



HRSDC is currently updating its privacy delegations to reflect the new Privacy Code and will include a new Delegation Order in its 2013–2014 Annual Report to Parliament on the Administration of the *Privacy Act*.

## **HRSDC’s Policy Framework for Integrated Privacy Management**

Given the importance of the protection of personal information in the context of emerging technologies and the potential implications for Canadians, the Department has adopted a comprehensive, risk-based and proactive approach to privacy management. This principle-based approach to privacy management was developed in 2011 in consultation with key stakeholders including the Treasury Board Secretariat, the Office of the Privacy Commissioner, the Office of the Information and Privacy Commissioner of Ontario and others. Using a Privacy by Design approach that emphasizes building privacy into the design and architecture of systems, technologies and business processes, the Framework includes the following key elements:

- **Governance and Accountability:** Roles, responsibilities and mechanisms to meet legal requirements, regulations, policies, standards and public expectations.
- **Stewardship of Personal Information:** Appropriate privacy protections to manage personal information through its life cycle.
- **Assurance of Compliance:** Formal processes and practices to ensure adherence to privacy specifications, policies, standards and laws.
- **Effective Risk Management:** Structured and coordinated activities to limit the probability and impact of negative events and maximize opportunities through risk identification, assessment and prioritization.
- **Culture, Training, and Awareness:** The promotion of a privacy-respectful culture ensures that employees, partners and delivery agents understand their privacy obligations and are aware of tools, resources, policies and processes related to privacy and personal information protection.

## **Privacy Governance at HRSDC**

HRSDC fosters governance and decision-making responsibilities for privacy through the Privacy and Information Security Committee and associated sub-committees.

## ***Privacy and Information Security Committee***

The mandate of the Privacy and Information Security Committee (PISC) is to support the coordination and prioritization of matters related to privacy and the protection of personal information; review and provide advice on portfolio-wide implications of significant privacy and personal information protection-related initiatives, including Privacy Impact Assessments and Information Sharing Agreements; oversee the development and implementation of key privacy policies and processes; and provide recommendations to the Deputy Minister on non-administrative uses of personal information (including, but not limited to, policy analysis, research and evaluation activities). PISC is co-chaired by the Corporate Secretary (who is also the Chief Privacy Officer) and the Departmental Security Officer.

PISC is supported by the following working groups:

- **Databank Review Working Group**

The Databank Review Working Group, a sub-committee of PISC, supports the application of privacy policy and the use of personal information for policy analysis, research and evaluation purposes. The working group regularly brings forward submissions to PISC relating to projects within the HRSDC portfolio for which it has been proposed that policy analysis, research and evaluation activities be conducted using personal information or linking of personal information databanks.

- **Departmental Security Working Group**

The Departmental Security Working Group strengthens preventive activities and facilitates the implementation of a consistent, integrated Security program throughout HRSDC's portfolio and its partners by developing tools to mitigate departmental security risks, including risks related to information, assets and services. By reinforcing collaboration between key security stakeholders, the working group facilitates an integrated approach and serves as a centre of expertise for strategic advice and tools related to security.

- **Departmental Engagement Working Group**

The newly formed Departmental Engagement Working Group consists of representatives from across the Department who meet regularly to discuss integrated awareness, training and engagement strategies, as well as policy guidance, regarding the stewardship of information assets. The horizontal integration of key enablers supporting the safeguarding and protection of information assets is a departmental priority. A risk-based, proactive strategy to engage the Department in cultural change supports

effective risk mitigation and contributes to excellence in the stewardship of departmental information assets.

## **Organization of the Privacy Function at HRSDC**

Privacy at HRSDC is corporately managed within the Corporate Secretariat at the national level by the Access to Information and Privacy (ATIP) Division and the Privacy Renewal Division. The Corporate Secretary leads the Corporate Secretariat and is the Chief Privacy Officer for the Department. Privacy at the regional level is led by Regional Privacy Coordinators.

### ***Access to Information and Privacy Division***

HRSDC's ATIP Division leads in administering access to information and privacy legislation for the HRSDC portfolio. A Director leads the ATIP Division and reports to the Corporate Secretary. The Director is supported by three managers who are responsible for the following units:

- The **Operations Unit** processes requests under the *Access to Information Act* and the *Privacy Act*. This includes performing a line-by-line review of records requested under this legislation. The Operations Unit is also the main point of contact with the Office of the Privacy Commissioner of Canada and the Office of the Information Commissioner of Canada for complaint resolution.
- The **Privacy Policy Management Unit** provides policy advice and guidance on the management of personal information (including the interpretation of the Department's Privacy Code) to officials of HRSDC across the portfolio. It provides advice on preparing Privacy Impact Assessments and assists program officials with drafting information-sharing agreements to ensure respect for privacy legislation and departmental policies. This Unit also responds to legal instruments requesting access to personal information held by the Department (e.g. subpoenas, court orders, search warrants) and liaises with the Office of the Privacy Commissioner on issues such as privacy incidents.
- The **Planning and Liaison Unit** develops products and tools, including standards and guidance to the Department on privacy issues. It leads on departmental access to information and privacy reporting to Parliament and central agencies, including business planning and preparation of annual reports. The Unit prepares and delivers privacy training and awareness sessions throughout the Department.

### ***Privacy Renewal Division***

The Privacy Renewal Division provides strategic advice to the Corporate Secretary as the Chief Privacy Officer on horizontal policy matters related to the modernization of privacy

management at HRSDC. A Director leads the Division and reports to the Corporate Secretary. The Division leads the Privacy Renewal Task Force and is tasked with the coordination and implementation of the Department's Privacy Renewal Action Plan. The Task Force is a horizontal interdisciplinary group composed of representatives from across branches with expertise in access to information and privacy, privacy and data protection policy, internal audit, IT security, business modernization and risk management and departmental security.

### ***Regional Privacy Coordinators***

While the ATIP Division has oversight and leadership responsibilities, the Department looks to its network of regional, local and branch coordinators to undertake many of its key privacy responsibilities. The majority of the thousands of *Privacy Act* requests that HRSDC receives in a typical year are processed by employees within HRSDC's regional offices. Regional privacy activities have been centralized under Regional Privacy Centres of Specialization to maintain capacity and expertise. HRSDC's Regional Privacy Centres of Specialization officers have delegated authority to process formal privacy requests under the *Privacy Act* and also process informal requests received by the Department. Under the functional direction of the Chief Privacy Officer, regional offices also provide privacy advice and guidance to regional management and members of the public.

## **Privacy Activities and Accomplishments for 2012–2013**

HRSDC's privacy management priorities for 2012–2013 focused on addressing both horizontal and vertical privacy risks within the Department. The horizontal risks refer to those corporate-level risks that apply to the Department more broadly, whereas the vertical privacy risks refer to those risks that fall within the domain of particular programs. HRSDC made important progress in its privacy renewal efforts in 2012–2013.

The trajectory of the Department's privacy renewal was altered by the two privacy incidents in 2012–2013 involving personal information, including the loss of an external hard drive from an HRSDC office in Gatineau, Quebec, which contained personal information of 583,000 Canada Student Loans Program borrowers between 2000 and 2006 and the loss of a USB key which contained the personal information of 5,045 Canada Pension Plan Disability appellants. These privacy incidents have focused attention on the importance of having robust information management practices, appropriate security safeguards, effective privacy protection and a strong departmental culture committed to the stewardship of information in the Department.

### **Action Plan on the Minister's Commitment to Information Security**

On January 11, 2013, in response to the privacy incidents, the Minister of Human Resources and Skills Development instructed the Department to adopt a series of measures to strengthen and improve the security and storage of personal information in the Department, including:

- new, stricter protocols to be implemented immediately (e.g. portable hard drives no longer permitted);
- immediate risk assessment of all portable security devices used in the Department to ensure appropriate safeguards are in place;
- mandatory training for all employees on the proper handling of sensitive information;
- implementation of new data loss prevention technology; and
- disciplinary measures that will be implemented for staff, up to and including termination.

### ***Departmental Response to Privacy Incidents***

HRSDC undertook actions to mitigate the impact on Canadians affected by the incidents. The Department initiated an awareness campaign to inform Canadians through public announcements, special information on Web pages, letters to affected individuals and a dedicated 1-800 toll-free information line to respond to questions concerning the security

incidents. The Department has notified those individuals, for which it has current contact information, if the Department notes any suspicious activity with respect to the client's Social Insurance Number.

Through an agreement with Equifax, the Department has offered, free of charge, a customized package of credit protection to individuals affected by the loss of the external hard drive and the USB key who consent to receive this service.

### ***USB Storage Devices Directive***

In 2012–2013, the Department established a new USB Storage Devices Directive. The Directive prohibits the use of unencrypted portable USB hard drives and USB keys on departmental computers. To implement the Directive, all USB keys were collected by the Department for proper disposal, and a limited number of encrypted USB keys were distributed to employees who regularly work with protected or classified information.

### ***Other Related Actions to Respond to Privacy Incidents***

Since the incidents, risk assessments have been conducted regarding all portable storage devices used in the Department's work environment to ensure that appropriate safeguards are in place. These assessments will continue on a regular, ongoing basis. New data loss prevention software technology is being implemented which will be configured to control or prevent the transfer of sensitive information.

The importance of the protection of personal information, including disciplinary consequences for non-compliance, has been and will continue to be communicated to all employees. All employees will be required to take new mandatory annual training to reinforce the critical importance of proper handling of sensitive personal information.

### **2012–2013 Privacy Renewal Action Plan**

The objective of HRSDC's multi-year Privacy Renewal Action Plan is to advance a comprehensive, risk-based, pro-active approach to privacy management and assurance to align and embed "privacy" as an enabler to the Department's transformation initiatives. The first phase of departmental privacy renewal activities (2011–2012) focused on the assessment of privacy risk and controls to inform the prioritization of departmental privacy action plans.

In 2012–2013, the second phase of the departmental privacy renewal activities reinforced the risk-based and proactive approach to privacy renewal. Key accomplishments included: establishment of Program-led Privacy Action Plans for eight of the Department's major statutory programs; development of a Departmental Directive on How to Respond to Security

Incidents Involving Personal Information; a review of privacy roles and responsibilities at all levels of the organization and the development of a renewed Departmental Policy on Privacy Management (to be implemented in 2013–2014); redesign of the Department’s Privacy Impact Assessment (PIA) process; privacy and information security training and awareness sessions; and establishment of the first-ever Privacy Awareness Week.

### ***Program-Led Privacy Action Plans***

Building upon the findings of the privacy risk assessments conducted in the first phase of the Privacy Renewal Action Plan, HRSDC developed Program-Led Action Plans to address privacy risks within eight of the Department’s major statutory programs. The objectives of the action plans are to mitigate privacy risks and to clearly articulate actions and expected outcomes, establish a timeline for completion and identify the involvement of key stakeholders involved in action plan implementation. These action plans reflect engagement of key stakeholders and corporate enablers within and across programs and clearly defined actions to mitigate potential residual privacy risks.

### ***Departmental Directive on How to Respond to Security Incidents Involving Personal Information***

In 2012–2013, HRSDC developed overarching security incident reporting protocols to ensure the consistent management of all security incidents within the portfolio. The protocols provide clear direction to departmental employees and their managers on their roles and responsibilities regarding the management of security incidents involving personal information that may result in a privacy breach.

### ***Departmental Policy on Privacy Management***

In 2012–2013, HRSDC conducted a review of its privacy policies, directives and guidance and engaged in consultations on a new Departmental Policy on Privacy Management with internal and external stakeholders, including the Treasury Board Secretariat and the Office of the Privacy Commissioner. The overarching objective of the proposed Departmental Policy on Privacy Management is to provide clear policy guidance and definition of roles and responsibilities within HRSDC on all privacy and privacy-related matters.

### ***Redesign of the Privacy Impact Assessment Process***

In 2012–2013, HRSDC redesigned its PIA process to identify and appropriately manage privacy risks related to new or substantially modified programs and activities. HRSDC continues to demonstrate compliance with privacy regulations and directives and has introduced a new structured and coordinated privacy risk assessment process. This collaborative,

multi-stakeholder process encompasses the identification, assessment and mitigation of privacy risks, framed within the broader risk management framework of the Department.

This redesign serves to streamline the PIA process, more effectively and efficiently identifying privacy risks associated with departmental initiatives and building comprehensive mitigation strategies, supported by action plans, to address these risks.

### ***Privacy Training and Awareness Strategy***

In 2012–2013, HRSDC developed an online course designed to provide basic introductory information related to privacy and access to information. This training tool was produced by Service Canada College @ HRSDC pedagogical experts in collaboration with subject matter experts from the ATIP Division. The online training module will be made available to all employees across the portfolio during the 2013-2014 fiscal year. New employees joining the Department will be required to complete this course.

In addition, the Department initiated the development of a mandatory integrated module in 2012–2013 that covers five disciplines related to the stewardship of information (security, IT security, information management, values and ethics and privacy). The integrated online training module is expected to be available to employees beginning in 2013-2014.

In addition, 14 joint awareness sessions with directorates across the Department were held in 2012–2013 with the Chief Privacy Officer, Departmental Security Officer and the Director General of Strategy, Planning, Architecture and Management in the Innovation and Information Technology Branch.

### ***Privacy Awareness Week at HRSDC***

In January 2013, the first annual HRSDC Privacy Awareness Week was held, which included corporate communications to all staff, a Deputy Minister's Blog, a speaker series featuring the Deputy Privacy Commissioner of Canada and the Chief Information Officer of the Government of Canada and kiosks at National Headquarters. Departmental officials responsible for privacy also contributed to various awareness weeks related to information management, security and IT security.

### ***Info Source Pilot Project***

During 2012–2013, HRSDC participated in the Treasury Board Secretariat's Info Source pilot project by posting its Info Source chapter on the departmental Internet site. HRSDC now has full control of its Info Source chapter and can ensure Canadians have access to accurate and



up-to-date information on Government of Canada programs by updating its content on an ongoing basis.

## **Privacy Performance Reporting for 2012–2013**

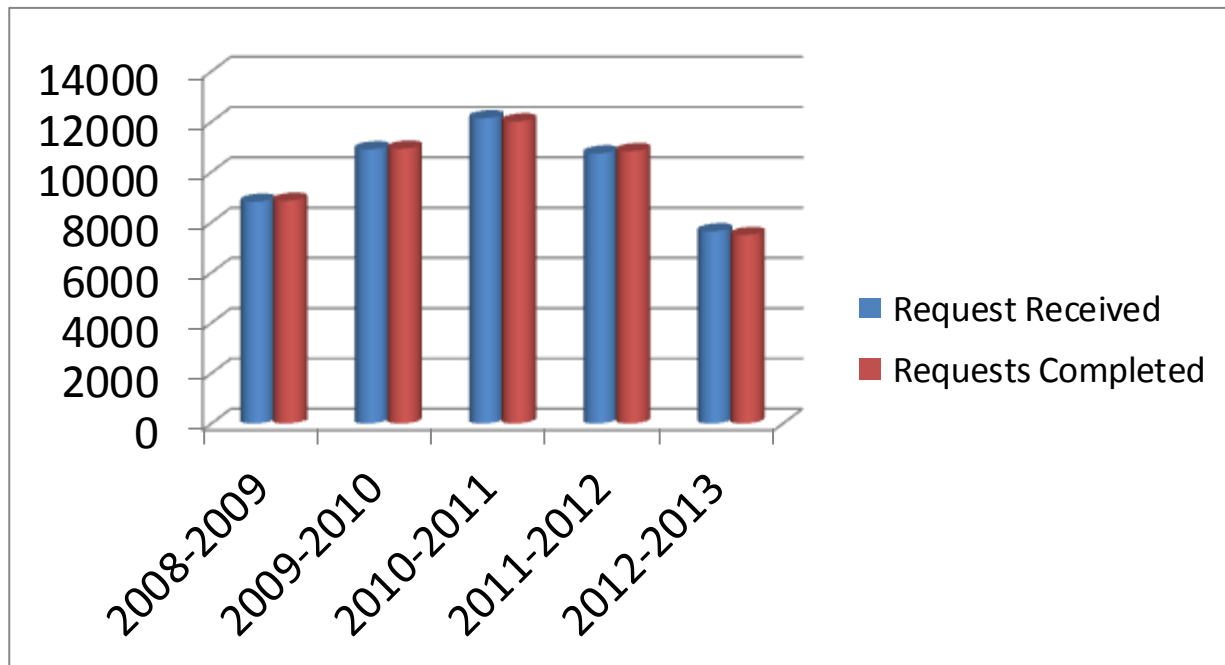
### **Requests for Information under the *Privacy Act***

The following is a summary of the information contained in the Statistical Report on the *Privacy Act* for 2012–2013, which is attached as Annex B.

Activity	2008–2009	2009–2010	2010–2011	2011–2012	2012–2013
Formal requests received under the <i>Privacy Act</i>	8,819	10,900	12,136	10,737	7,639
Requests completed during the year	8,858	10,927	12,010	10,830	7,493
Requests completed within 30 calendar days	8,032	9,493	10,179	9,944	6,315
Requests completed within 31 to 60 calendar days	535	1,298	1,776	732	1,002
Requests completed within 61 or more calendar days	291	136	55	154	176
Complaints to Privacy Commissioner of Canada	125	16	17	24	17
Privacy Impact Assessments forwarded to the Office of the Privacy Commissioner	0	9	1	6	6
Disclosures in the Public Interest	5	26	35	78	121

### ***Requests***

***Privacy Act* Requests Received and Completed**

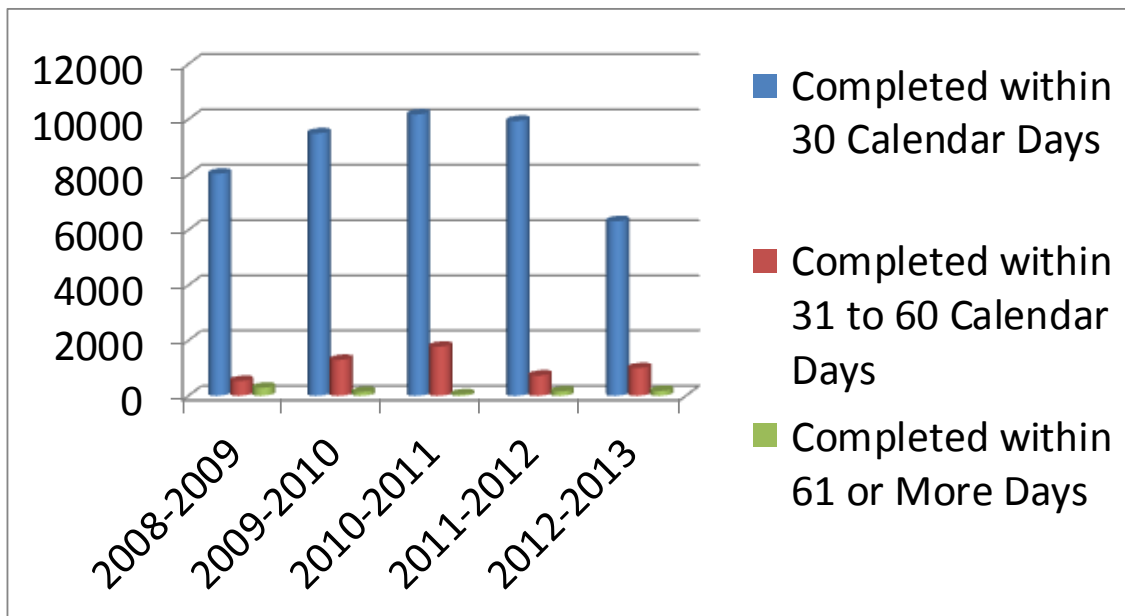


In the last five fiscal years, the number of requests received by HRSDC increased from 2008–2009 to 2010–2011. The number of formal requests to the Department declined in 2011–2012 and 2012–2013.

In 2012–2013, HRSDC received 7,639 requests under the *Privacy Act* and completed 7,493 requests, which includes requests received before the reporting period. Typical privacy requests are from clients seeking to obtain a copy of their Canada Pension Plan file, their Old Age Security file, the contents of their Employment Insurance file or their Canada Student Loans file, as well as from employees seeking to obtain a copy of their personnel information.

Of the requests that were completed in 2012–2013, 90% resulted in at least a partial release of records to the applicant. The remaining 10% of requests fell into categories of “No records exist” and “Request abandoned.”

### ***Privacy Act* Requests by Calendar Days Taken to Complete**



In the last five fiscal years, the majority of requests were completed within 30 calendar days.

In 2012–2013, 84% of requests were responded to within the first 30 calendar days, with 49% of requests receiving a response in the first 15 days. More than 97% of requests were processed within the first 60 days.

For the requests where an exemption was invoked, the common provision used was section 26 of the *Privacy Act*, which was applied to 4,642 requests. This provision seeks to protect personal information pertaining to individuals other than the requester.

The format of information released was paper for 6,260 requests and electronic for 457.

## ***Pages***

In 2012–2013, a total of 559,428 pages were reviewed (processed). Of these, 515,769 pages, or 92%, were disclosed (in whole or in part) to the requester. The remaining 8% were either withheld pursuant to one of the *Privacy Act*'s exemption provisions or not released because the corresponding request was abandoned by the requester.

Of the pages reviewed, 6,720 requests, or 90%, involved processing 500 pages or less, with 5,281 requests requiring the review of 100 pages or less and 1,439 requests requiring a review of between 101 and 500 pages. While 32 requests, or 0.4%, required a review of more than 1,000 pages; this work resulted in the disclosure of 53,438 pages, or 9% of all pages disclosed.

## ***Other Complexities***

In addition to information regarding the number of pages processed, the Statistical Report contains information regarding “Other Complexities,” namely the number of requests where consultations are required, where legal advice was sought and where interwoven information exists. The Treasury Board Secretariat defines requests containing “interwoven information” as those “where the relevant records contain personal information about another individual that is interwoven with the personal information of the requester.” The category “Other,” according to the Treasury Board Secretariat, “comprises high profile subject matter, requests where records are in a region or other country, and requests where the records are in a language other than English or French.”

Consultations were required on 16 requests. Legal advice was not sought on the processing of any *Privacy Act* request that was completed in 2012–2013. A total of 175 requests contained interwoven information. Finally, 5,878 requests were processed in the regions and therefore fall into the category “Other.”

## ***Performance***

In 2012–2013, the Department was unable to meet its deadline for 990 requests, representing 13% of requests processed; these figures represent a decrease in performance from 2011–2012, when the Department was unable to meet its deadline for 513 requests, representing just under 5% of requests processed. The common reason for missing the deadline was “Other” (53% – mainly due to difficulties in obtaining relevant records). Two requests were late due to internal or external consultations. In 835 cases, the Department was late by 30 days or less, and 34 requests were late by more than 120 days.

### ***Extensions***

An extension of up to 30 days beyond the initial period is permitted if responding to the request would unreasonably interfere with operations or if external consultations are required. In addition, an extension can be claimed for translation purposes or to convert a record in another format. (Translation/conversion extensions are not limited to a 30-day maximum, as is the case for interference with operations and consultation extensions.) In 2012–2013, HRSDC claimed an extension on 166 requests. This represents an increase from 2011–2012, when the Department claimed extensions on 116 requests.

### ***Translation of Records***

The records released in response to two requests were translated, as requested by the applicants. One set of records was translated from English to French, and the other was translated from French to English.

### ***Requests for Correction of Information***

Individuals have a right to request correction of any erroneous personal information pertaining to them, so long as the individuals can adequately substantiate their cases. Three requests for correction of personal information were received in 2012–2013. One was accepted and two requests were denied to applicants who were unable to adequately support their claims that information pertaining to them was erroneous.

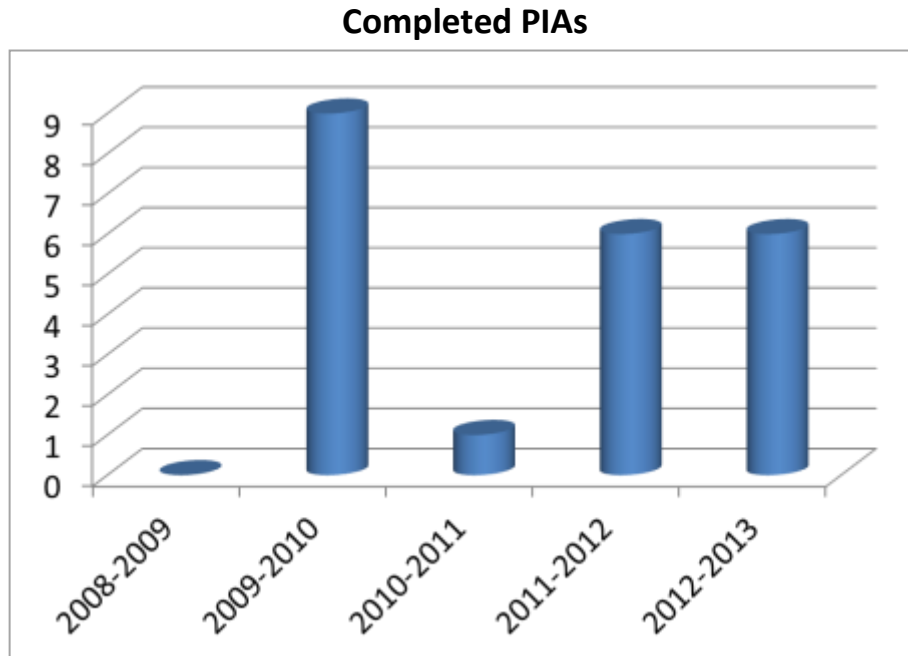
### ***Consultations Received by HRSDC***

HRSDC responded to 20 consultations in 2012–2013, 17 of which were received from other federal institutions and three from another level of government, corresponding to a review of 760 pages. Five of these consultations resulted in a recommendation to entirely disclose the records, with nine counselling the consulting department or organization to disclose in part. In one consultation, HRSDC recommended that the records be exempted entirely, while for the remaining five consultations the recommendation was “Other.” Consultations with the Privy Council Office on Cabinet Confidences were not required during the reporting period.

### ***Financial Considerations***

In 2012–2013, the Department spent over \$3.8 million on salaries associated with administering the *Privacy Act* as well as \$59,000 on overtime. Non-salary costs amounted to about \$111,000, for a total of about \$4.0 million. In 2012–2013, 32.3 full-time equivalents (FTEs) in the regions and 28 FTEs at National Headquarters were involved in the administration of the *Privacy Act*.

## Completed Privacy Impact Assessments



According to the Treasury Board Secretariat (TBS), “A Privacy Impact Assessment (PIA) is not considered to be completed until the final, approved copy...has been sent to both the Office of the Privacy Commissioner and to the Information and Privacy Policy Division, Treasury Board Secretariat.” Based on the standard as set out by TBS, HRSDC completed six PIAs in 2012–2013:

### 1. Connecting Canadians with Available Jobs

The Connecting Canadians with Available Jobs initiative was first announced in May 2012. It is a strategic intervention that seeks to fulfill the Department’s mandate to adjust its policies and programs so that its learning and employment programs continue to meet Canadians' changing needs and respond to the rapidly changing global economy.

The initiative consists of the following five components:

- modifications to the Employment Insurance (EI) legislation and regulations;
- providing increased labour market information to Canadians;
- enhancing integrity measures to ensure claimants are fulfilling their obligations under the new regulations;
- changing the Temporary Foreign Worker Program to ensure employers consider Canadians prior to hiring temporary foreign workers; and
- conducting negotiations with the provinces/territories on projects that would enable earlier interventions with EI claimants.

## **2. Cyber-Authentication Renewal – Phase I**

The purpose of Phase I of the Cyber-Authentication Renewal (CAR) initiative is to implement the changes required within HRSDC to prepare for and leverage the SecureKey Concierge credential service solution. Over time, the modifications implemented as a part of CAR Phase I are expected to increase client use of the online service channel for HRSDC programs.

## **3. Cyber-Authentication Renewal – Phase II**

The purpose of Phase II of the Cyber-Authentication Renewal (CAR) initiative is to implement the changes required within HRSDC to prepare for and leverage the GCKey credential service solution. Over time, the modifications implemented as a part of CAR Phase II are expected to increase client use of the online service channel for HRSDC programs.

## **4. Federal Income Support for Parents of Murdered and Missing Children**

Effective January 1, 2013, the Federal Income Support for Parents of Murdered or Missing Children grant provides \$350 per week of income support for up to 35 weeks to parents of murdered or missing children (less than 18 years of age) whose death or disappearance is the result of a probable *Criminal Code* offence. Applicants must apply for and receive the grant within one year of the offence and may only apply for the grant once within that one-year period. The maximum 35 weeks of benefits available may be shared by more than one eligible applicant for the same incident.

## **5. Old Age Security Proactive Enrolment Initiative**

The objective of the Old Age Security (OAS)/Guaranteed Income Supplement (GIS) Service Improvement Strategy is to improve service to a growing number of seniors in ways that can generate efficiencies for individuals and government. A key element of the Strategy is the OAS Proactive Enrolment Initiative, which will encompass both the automatic enrolment process and a streamlined process for many seniors at age 65. This will improve service delivery by reducing the administrative burden on Canadians, enhancing administrative efficiencies and offsetting projected increases in workload.

## **6. Social Security Tribunal**

The new Social Security Tribunal (SST) replaces the four legacy administrative tribunals and provides a common, independent quasi-judicial appeal process for government decisions on Employment Insurance (EI), Canada Pension Plan (CPP) and Old Age Security (OAS) program benefits. The SST opened on April 1, 2013, and comprises

Governor-in-Council-appointed decision-makers (i.e. “members”) who will be supported by HRSDC (i.e. “the Department”) management, operational, financial, administrative, legal and medical staff. The legacy tribunals will wind down their operations over 2013/2014 and, as of April 1, 2014, the SST will be the only tribunal responsible for EI, CPP and OAS appeals.

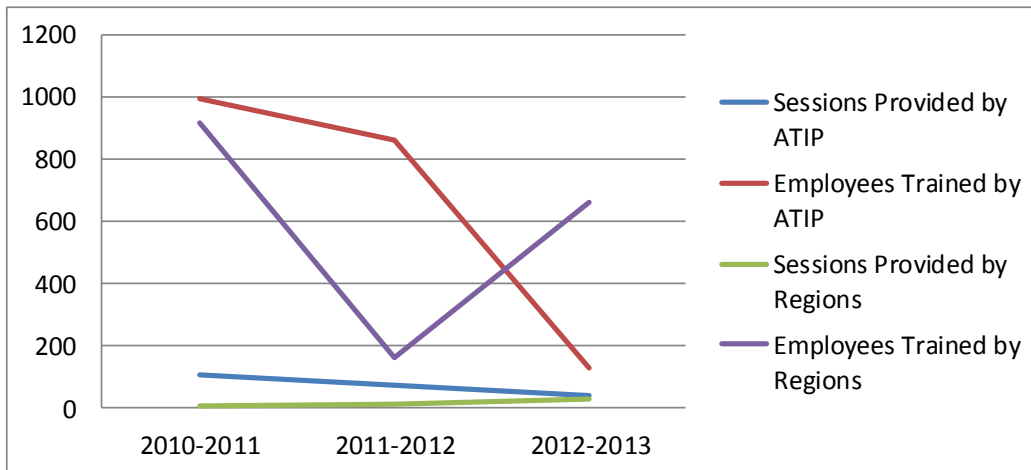
### *PIA Summaries*

Summaries of the six PIAs completed by HRSDC in 2012-2013 are available on the departmental website at the following address:

[http://www.hrsdc.gc.ca/eng/transparency/ati/reports/pia/2012\\_2013.shtml](http://www.hrsdc.gc.ca/eng/transparency/ati/reports/pia/2012_2013.shtml)

## Privacy Training and Awareness Activities

### In-Person Privacy Training



Within HRSDC, privacy training is delivered at National Headquarters and in the regions by the ATIP Division. Further privacy and job-specific training in the regions is provided by the Regional Privacy Centres of Specialization. Regional Privacy Centres of Specialization also work closely with the other regional business lines to develop ATIP tools for staff.

In 2012–2013, the ATIP Division provided 36 training sessions on access to information and privacy issues and awareness to 125 employees at National Headquarters. In addition, the officials responsible for privacy in the regions provided 27 sessions to 662 employees in the regions.

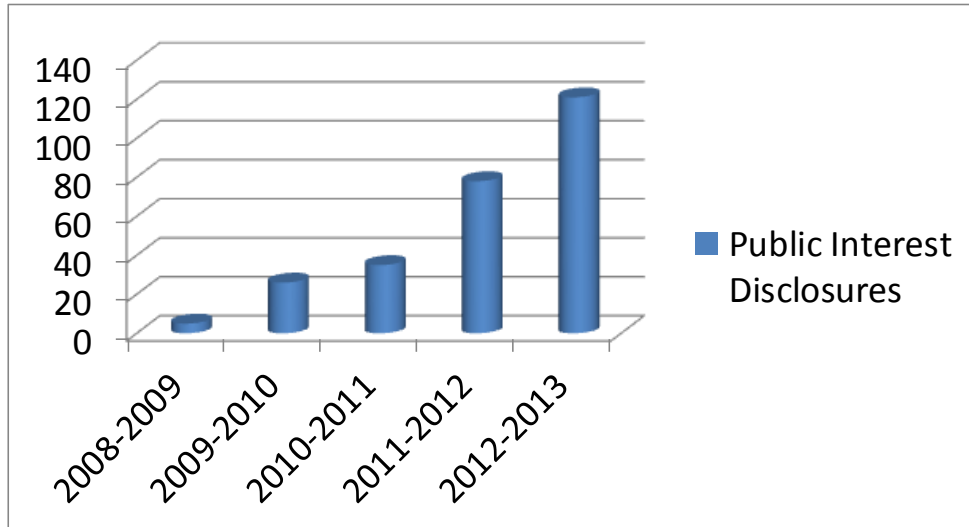
Overall, provision of in-person privacy training has declined over the past three fiscal years as the Department transitions to an online, self-directed learning model, not only for privacy but



also for access to information, security, IT security, information management and values and ethics.

## Public Interest Disclosures

**Public Interest Disclosures**

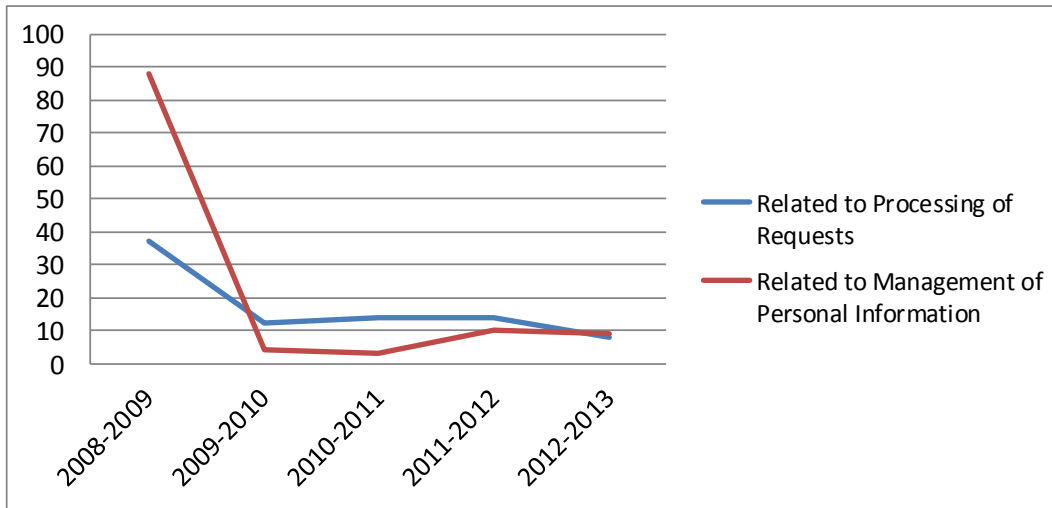


Under subsection 37(1) of the DHRSD Act, the Department may disclose personal information under its control “if the Minister is of the opinion that the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure or that disclosure would clearly benefit the individual to whom the information relates.”

In 2012–2013, the Department made 121 public interest disclosures under subsection 37(1) of the DHRSD Act. Where possible, the Office of the Privacy Commissioner (OPC) is notified in advance of the disclosure. Of the 121 public interest disclosures, seven were reported to the OPC. The remaining 114 public interest disclosures which occurred in 2012–2013 were reported to the OPC after the closure of the reporting period.

## Complaints and Investigations

### Privacy Complaints to the Office of the Privacy Commissioner



In four of the last five fiscal years, the number of complaints to the Office of the Privacy Commissioner has remained relatively stable. The exception is 2008–2009, when the number of privacy complaints reached 125.

In 2012–2013, the Department was notified of 17 complaints received by the Office of the Privacy Commissioner. Of these cases, eight related to the processing of *Privacy Act* requests—for example, the application of exemptions and the time taken to provide a response. The remaining nine complaints related to HRSDC’s handling of personal information—for example, allegations of improper use, collection or disclosure of personal information.

HRSDC received findings on 14 complaints in 2012–2013. The Office of the Privacy Commissioner ruled that two complaints were not well-founded and that seven complaints were well-founded. Two complaints were discontinued, two were settled in the course of the investigation and one complaint was resolved.

These complaints did not lead to a change in policies and procedures.

## **Moving Forward in 2013–2014**

As the Department moves forward on its privacy renewal agenda in 2013–2014, it will continue to implement its Privacy Renewal Action Plan with adjustments to address changes in the strategic and operating environment.

Areas of particular focus for 2013–2014 will include finalizing and implementing the Departmental Policy on Privacy Management, finalizing renewal of the privacy accountability framework, ingraining and deepening privacy and information security responsibilities in its organizational culture, a proactive and coordinated privacy and information security risk management approach and continued enhancements of HRSDC's management and protection of departmental information assets.

In addition, the Department will provide customized credit protection from TransUnion Canada to individuals who may have been affected by the security incidents. This credit protection will, along with services already provided by Equifax Canada, provide additional, reliable safeguarding of credit files, including alert messages that provide notification that personal information of affected individuals may have been compromised.

While strategies and action plans are important and necessary, a culture of privacy protection is also critical to the Department's privacy management success. Enhancing, maintaining and nurturing a culture of privacy and security awareness will require everyone's participation.

## Annex A: Delegation Order

### ORDONNANCE DE DÉLÉGATION DE POUVOIRS

#### RESSOURCES HUMAINES ET DÉVELOPPEMENT DES COMPÉTENCES

En vertu de l'article 11 de la *Loi sur le ministère des Ressources humaines et du Développement des compétences*, de l'article 17 de la *Loi sur le ministère du Développement social* et de l'article 73 de la *Loi sur la protection des renseignements personnels*, la ministre des Ressources humaines et du Développement des compétences délègue, par les présentes, aux personnes, cadres ou employés qui occupent les postes mentionnés en annexe au ministère des Ressources humaines et du Développement des compétences, ou aux personnes, cadres ou employés occupant ces postes à titre intérimaire, les attributions de la ministre ou du responsable de l'institution, comme il est indiqué en annexe.


- *Partie 4 de la Loi sur le ministère des Ressources humaines et du Développement des compétences*
- *Partie 2 de la Loi sur le ministère du Développement social*
- *Loi sur la protection des renseignements personnels*

### DELEGATION ORDER

#### HUMAN RESOURCES AND SKILLS DEVELOPMENT

The Minister of Human Resources and Skills Development, pursuant to section 11 of the *Department of Human Resources and Skills Development Act*, section 17 of the *Department of Social Development Act* and section 73 of the *Privacy Act* hereby designates the persons, officers or employees holding the positions with Human Resources and Skills Development set out in the schedules attached hereto, or the persons, officers or employees occupying on an acting basis those positions, to exercise the powers or perform the duties or functions of the Minister or to exercise or perform the powers, duties or functions of the head of the institution, as specified in the attached schedules.

- *Part 4 of the Department of Human Resources and Skills Development Act*
- *Part 2 of the Department of Social Development Act*
- *Privacy Act*

  
Ministre des Ressources humaines et du  
Développement des compétences / Minister of  
Human Resources and Skills Development

AUG 17 2010  
date

**Department of Human Resources and Skills Development Act  
And Department of Social Development Act**

Delegated Officials	Delegated Authority	Department of Human Resources and Skills Development Act provision	Department of Social Development Act provision
Deputy Minister, HRSD  Senior Associate Deputy Minister/ Chief Operating Officer  Associate Deputy Minister  Corporate Secretary  Director, Access to Information and Privacy (ATIP)	<i>Determining the conditions under which the information may be made available to an individual or their representative or to a member of Parliament inquiring on behalf of an individual.</i>	33(2)	27(2)
Deputy Minister, HRSD	<i>Determining whether it is advisable to make information available, and agreeing to the conditions under which information may be made available, to a minister or a public officer of a prescribed federal institution for the administration or enforcement of a prescribed federal or provincial law or activity</i>	35(2)	29(2)
Deputy Minister, HRSD	<i>Determining whether it is advisable for the minister or a public officer of a prescribed federal institution to which information was made available under 35(2) of the DHRSD Act or 29(2) of the DSD Act to make that information available for the same purpose, and agreeing to the conditions under which that information may be made available, to any other person or body</i>	35(3)	29(3)

Deputy Minister, HRSD	<i>Determining whether it is advisable to make information available, and agreeing to the conditions under which the information may be made available, to the government of a province, or to a public body created under the law of a province, for the administration or enforcement of a federal law or activity or a provincial law</i>	36(1)	30(1)
Deputy Minister, HRSD	<i>Determining whether it is advisable to make information available, and agreeing to the conditions under which the information may be made available, to the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the administration or enforcement of a law.</i>	36(2)	30(2)
Deputy Minister, HRSD	<i>Determining whether it is advisable for a government, public body, organization or institution to which information was made available under subsec. 36(1) or (2) of the DHRSD Act or 29(1) or (2) of the DSD Act to make that information available for the same purpose, and agreeing to the conditions under which that information may be made available, to any other person or body</i>	36(3)	30(3)
Deputy Minister, HRSD Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary	<i>Determining whether the public interest in disclosing the information clearly outweighs any invasion of privacy that could result from the disclosure or determining whether disclosure would clearly benefit the individual to whom the information relates.</i>	37(1)	31(1)

<p>Director, ATIP</p> <p><b>For only those situations where there is a threat to the safety and/or security of an individual:</b></p> <p>Departmental Security Officer</p> <p>Regional Security Officers</p> <p>Regional Privacy Coordinators</p> <p>Service Area Managers</p> <p>Call Centre Managers</p> <p>Manager, Corporate Security</p> <p>Security Advisor, Corporate Security</p>			
<p>Deputy Minister, HRSD</p> <p>Senior Associate Deputy Minister/ Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p>	<p><i>Authority to notify the Privacy Commissioner</i></p>	<p>37(2)</p>	<p>31(2)</p>
<p>Deputy Minister, HRSD</p>	<p><i>Determining whether the disclosure for research or statistical purposes to any person or body, is consistent with the principles set out in paragraphs 39(1)a) to e) of the DHRSD Act or in paragraphs 33(1)(a) to (e) of the DSD Act.</i></p>	<p>38(a)</p>	<p>32(a)</p>
<p>Deputy Minister, HRSD</p>	<p><i>Determining whether the research or statistical purpose for which information is to be made available to any person or body cannot reasonably be accomplished unless the information is provided in a form that may identify the individual to whom the information relates</i></p>	<p>38(b)</p>	<p>32(b)</p>

Deputy Minister, HRSD	<i>Determining the conditions under which the information may be made available for research or statistical purposes to any person or body</i>	38(c)	32(c)
Deputy Minister, HRSD Senior Assistant Deputy Minister Strategic Policy and Research	<i>Authorizing a public officer to use information for the purpose of policy analysis, research or evaluation when the information would allow an individual to be identified.</i>	39(2)	33(2)
<b><u>CRIMINAL:</u></b> Deputy Minister, HRSD Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP  <b><u>CIVIL:</u></b> Deputy Minister, HRSD Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP ADM, Ontario Region Regional Executive Heads Regional Privacy Coordinators	<i>Determining whether it is appropriate for the Minister, members of the Employment Insurance Commission, or public officers to give, in connection with any legal proceedings, evidence relating to information that is privileged under s. 32 of the DHRSD Act or under s. 26 of the DSD Act or to produce a statement or other writing containing any such privileged information</i>	40	34



**Note:** The following delegation is limited to the collection of information:

<b>Delegated Officials</b>	<b>Delegated Authority</b>	<b><i>Department of Human Resources and Skills Development Act provision</i></b>	<b><i>Department of Social Development Act provision</i></b>
Deputy Minister, HRSD	<i>Authority to enter into agreements to obtain information for the administration or enforcement of a program with federal institutions, governments of provinces or public bodies created under provincial law, governments of foreign states, international organizations of states or international organizations established by the governments of states, any institution of any such government or organization, and other persons or bodies</i>	41	35

***Privacy Act – Delegation of Authority***  
***Human Resources and Skills Development Canada***

Description	Section	Delegated Authority
Approval to disclose for research or statistical purposes	8(2)(j)	Deputy Minister
Approval to disclose personal information when the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure or the disclosure would clearly benefit the individual to whom the information relates	8(2)(m)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p><b>For those situations where there is a threat to the safety and/or security of an individual:</b></p> <p>Departmental Security Officer</p> <p>Regional Security Officers</p> <p>Regional Privacy Coordinators</p> <p>Service Area Managers</p> <p>Call Centre Managers</p> <p>Manager, Corporate Security</p> <p>Security Advisor, Corporate Security</p>
Retention of a record of requests and disclosed records to investigative bodies under section 8(2)(e) of the <i>Privacy Act</i> .	8(4)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p>

		<p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Senior Public Rights Officer, ATIP</p> <p>Public Rights Officer, ATIP</p> <p>Public Rights Analyst, ATIP</p> <p>Regional Privacy Coordinators</p>
Notification of the Privacy Commissioner of all disclosures made under paragraph 8(2)(m) of the <i>Privacy Act</i> (public interest).	8(5)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p>
Retention of records of uses of personal information	9(1)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p>
Notification of the Privacy Commissioner of any new consistent uses of personal information and ensure use is included in next statement of consistent uses set forth in the Index	9(4)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p>

<p>Include personal information in personal information banks</p>	<p>10(1)</p>	<p>Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP</p>
<p>Respond to request for access within 30 days and give written notice and, if access to be given, give access.</p>	<p>14</p>	<p>Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Senior Public Rights Officer, ATIP Public Rights Officer, ATIP Public Rights Analyst, ATIP Regional Privacy Coordinators Positions as per Annex A</p>
<p>Extension of the 30 day time limit to respond to a privacy request.</p>	<p>15</p>	<p>Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Senior Public Rights Officer, ATIP Public Rights Officer, ATIP</p>

		Public Rights Analyst, ATIP Regional Privacy Coordinators Positions as per Annex A
Decision on whether to translate a response to a privacy request in one of the two official languages.	17(2)(b)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Senior Public Rights Officer, ATIP Public Rights Officer, ATIP Public Rights Analyst, ATIP Regional Privacy Coordinators Positions as per Annex A
Decision on whether to convert information to an alternate format	17(3)(b)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Senior Public Rights Officer, ATIP Public Rights Officer, ATIP Public Rights Analyst, ATIP

		Regional Privacy Coordinators Positions as per Annex A
Decision to refuse to disclose information contained in an exempt bank.	18(2)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP
Decision to refuse access to information that was obtained in confidence from the government of a foreign state or institution, an international organization of states or an institution thereof, the government of a province or institution thereof, a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government, or the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the Westbank First Nation Self-Government Act.	19(1)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Regional Privacy Coordinators
Authority to disclose information referred to in 19(1) if the government, organization or institution described in 19(1) consents to the disclosure or makes the information public.	19(2)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP

		<p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Regional Privacy Coordinators</p>
<p>Refuse to disclose information that may be injurious to the conduct of federal-provincial affairs</p>	20	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p>
<p>Refuse to disclose information that may be injurious to international affairs or the defence of Canada or one of its allies.</p>	21	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p>
<p>Refuse to disclose information prepared by an investigative body, information injurious to the enforcement of a law, or information injurious to the security of penal institutions</p>	22	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Senior Public Rights Officer, ATIP</p>

		<p>Public Rights Officer, ATIP</p> <p>Public Rights Analyst, ATIP</p> <p>Regional Privacy Coordinators</p> <p>Positions as per Annex A</p>
<p>Refuse to disclose information prepared by an investigative body for security clearance.</p>	23	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Regional Privacy Coordinators</p>
<p>Refuse to disclose information that was collected by the Canadian Penitentiary Service, the National Parole Service or the National Parole Board while the individual was under sentence if the conditions in the section are met</p>	24	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Regional Privacy Coordinators</p>
<p>Refuse to disclose information which could threaten the safety of individuals</p>	25	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p>



		Managers, ATIP Senior Public Rights Administrator, ATIP
Refuse to disclose information about another individual and shall refuse to disclose such information where disclosure is prohibited under section 8	26	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Senior Public Rights Officer, ATIP Public Rights Officer, ATIP Public Rights Analyst, ATIP Regional Privacy Coordinators Positions as per Annex A
Refuse to disclose information that is subject to solicitor-client privilege.	27	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Regional Privacy Coordinators
Refuse to disclose information relating to the individual's physical or mental health where the disclosure is contrary to the best interests of the individual	28	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister

		<p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Regional Privacy Coordinators</p>
Receive notice of investigation by the Privacy Commissioner	31	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p>
Right to make representations to the Privacy Commissioner during an investigation	33(2)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Senior Public Rights Officer, ATIP</p> <p>Public Rights Officer, ATIP</p> <p>Public Rights Analyst, ATIP</p> <p>Regional Privacy Coordinators</p>
Receive Privacy Commissioner's report of findings of an investigation and give notice of action taken	35(1)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p>

		<p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Senior Public Rights Officer, ATIP</p> <p>Public Rights Officer, ATIP</p> <p>Public Rights Analyst, ATIP</p> <p>Regional Privacy Coordinators</p>
<p>Provision of addition information to a complainant after receiving a 35(1)(b) notice.</p>	35(4)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p> <p>Senior Public Rights Administrator, ATIP</p> <p>Senior Public Rights Officer, ATIP</p> <p>Public Rights Officer, ATIP</p> <p>Public Rights Analyst, ATIP</p> <p>Regional Privacy Coordinators</p>
<p>Receive Privacy Commissioner's report of findings of investigation of exempt bank</p>	36(3)	<p>Deputy Minister</p> <p>Senior Associate Deputy Minister/Chief Operating Officer</p> <p>Associate Deputy Minister</p> <p>Corporate Secretary</p> <p>Director, ATIP</p> <p>Managers, ATIP</p>

<p>Receive report of Privacy Commissioner's findings after compliance investigation</p>	<p>37(3)</p>	<p>Deputy Minister                  Senior Associate Deputy Minister/Chief Operating Officer                  Associate Deputy Minister                  Corporate Secretary                  Director, ATIP                  Managers, ATIP</p>
<p>Request that a court hearing, undertaken with respect to certain sections of the Act, be held in the National Capital Region.</p>	<p>51(2)(b)</p>	<p>Deputy Minister                  Senior Associate Deputy Minister/Chief Operating Officer                  Associate Deputy Minister                  Corporate Secretary                  Director, ATIP                  Managers, ATIP</p>
<p>Request and be given right to make representations in section 51 hearings</p>	<p>51(3)</p>	<p>Deputy Minister                  Senior Associate Deputy Minister/Chief Operating Officer                  Associate Deputy Minister                  Corporate Secretary                  Director, ATIP                  Managers, ATIP</p>
<p>Prepare annual report to Parliament</p>	<p>72(1)</p>	<p>Deputy Minister                  Senior Associate Deputy Minister/Chief Operating Officer                  Associate Deputy Minister                  Corporate Secretary                  Director, ATIP</p>

## ANNEX A

### POSITIONS DELEGATED IN THE REGIONS, AS NOTED IN THE DELEGATION INSTRUMENT

#### Atlantic Region

No additional positions identified

#### Québec Region

<b>Title</b>	<b>Position number</b>	<b>Sections</b>
<i>Regional Office</i>		
Project Lead, Access to Information and Privacy (Public Rights)	29737	14, 15, 17(2)(b), 17(3)(b), 22, 26
Advisor, Access to Information and Privacy (Public Rights)	24448	14, 15, 17(2)(b), 17(3)(b), 22, 26

#### Ontario Region

<b>Title</b>	<b>Position number</b>	<b>Sections</b>
<i>Regional Office</i>		
Access to Information and Privacy (ATIP) Officer	54687	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28
Team Leader	59839	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28
ATIP Officer	40700 (bil)	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28
ATIP Officer	54688 (bil)	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28

ATIP Officer	53113	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28
ATIP Officer	53112	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28

### Western Canada and Territories Region

<b>Title</b>	<b>Position number</b>	<b>Sections</b>
<i>Regional Offices</i>		
Official Languages and Public Rights Officer	67433	14, 15, 17(2)(b), 17(3)(b), 22, 26
Communications Officer	52807	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program Officer	75661	14, 15, 17(2)(b), 17(3)(b), 22, 26
Regional Access to Information and Privacy (ATIP) Officer	49263	14, 15, 17(2)(b), 17(3)(b), 22, 26
<i>Local Offices</i>		
Strategic Planning/Continuous Improvement Consultant	43611	14, 15, 17(2)(b), 17(3)(b), 22, 26
Service Canada Benefit Officer	76691	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	76609	14, 15, 17(2)(b), 17(3)(b), 22, 26
Team Leader	76280	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	69517	14, 15, 17(2)(b), 17(3)(b), 22, 26
Service Canada Benefit	70255	14, 15, 17(2)(b), 17(3)(b), 22, 26

Officer		
Service Canada Benefit Officer	75411	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	74949	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	74043	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	74154	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	76079	14, 15, 17(2)(b), 17(3)(b), 22, 26
Service Canada Benefit Officer	71724	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	69487	14, 15, 17(2)(b), 17(3)(b), 22, 26
Service Canada Benefit Officer	66706	14, 15, 17(2)(b), 17(3)(b), 22, 26
Service Canada Benefit Officer	67988	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	48612	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	48127	14, 15, 17(2)(b), 17(3)(b), 22, 26
Team Leader	66148	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	72470	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	52549	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service	67205	14, 15, 17(2)(b), 17(3)(b), 22, 26

Delivery Clerk		
Program and Service Delivery Clerk	67612	14, 15, 17(2)(b), 17(3)(b), 22, 26
Program and Service Delivery Clerk	75255	14, 15, 17(2)(b), 17(3)(b), 22, 26
Payment Service Officer	68379	14, 15, 17(2)(b), 17(3)(b), 22, 26



## Annex B: Statistical Report on the *Privacy Act*



Government of Canada / Gouvernement du Canada

### Statistical Report on the *Privacy Act*

Name of institution: Human Resources and Skills Development Canada

Reporting period: 01/04/2012 to 31/03/2013

#### **PART 1 – Requests under the *Privacy Act***

	Number of Requests
Received during reporting period	7369
Outstanding from previous reporting period	369
<b>Total</b>	<b>7738</b>
Closed during reporting period	7493
Carried over to next reporting period	245

#### **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	577	747	626	57	10	5	0	2022
Disclosed in part	2541	1732	329	65	17	10	2	4696
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
No records exist	474	122	41	6	1	1	0	645
Request abandoned	82	40	6	0	2	0	0	130
<b>Total</b>	<b>3874</b>	<b>2641</b>	<b>1002</b>	<b>128</b>	<b>30</b>	<b>16</b>	<b>2</b>	<b>7493</b>

##### 2.2 Exemptions

Section	Number of requests	Section	Number of requests	Section	Number of requests
18(2)	0	22(1)(a)(i)	1	23(a)	1
19(1)(a)	0	22(1)(a)(ii)	0	23(b)	0
19(1)(b)	1	22(1)(a)(iii)	0	24(a)	0
19(1)(c)	1	22(1)(b)	28	24(b)	0
19(1)(d)	0	22(1)(c)	0	25	10
19(1)(e)	0	22(2)	1	26	4642
19(1)(f)	0	22.1	1	27	26
20	0	22.2	0	28	1
21	1	22.3	0		

### 2.3 Exclusions

Section	Number of requests	Section	Number of requests	Section	Number of requests
69(1)(a)	0	70(1)(a)	0	70(1)(d)	0
69(1)(b)	0	70(1)(b)	0	70(1)(e)	0
69.1	0	70(1)(c)	0	70(1)(f)	0
				70.1	0

### 2.4 Format of information released

Disposition	Paper	Electronic	Other formats
All disclosed	1987	35	0
Disclosed in part	4273	422	1
<b>Total</b>	<b>6260</b>	<b>457</b>	<b>1</b>

### 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	44715	44715	2022
Disclosed in part	512614	471054	4696
All exempted	0	0	0
All excluded	0	0	0
Request abandoned	2099	0	130

#### 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	1886	19190	126	17263	8	5876	2	2386	0	0
Disclosed in part	3268	126439	1312	238459	87	55104	27	34494	2	16558
All exempted	0	0	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0	0	0
Abandoned	127	0	1	0	1	0	1	0	0	0
<b>Total</b>	<b>5281</b>	<b>145629</b>	<b>1439</b>	<b>255722</b>	<b>96</b>	<b>60980</b>	<b>30</b>	<b>36880</b>	<b>2</b>	<b>16558</b>

2.5.3 Other complexities

Disposition	Consultation required	Legal Advice Sought	Interwoven Information	Other	Total
All disclosed	0	0	0	1082	1082
Disclosed in part	16	0	175	4554	4745
All exempted	0	0	0	0	0
All excluded	0	0	0	127	127
Abandoned	0	0	0	115	115
<b>Total</b>	<b>16</b>	<b>0</b>	<b>175</b>	<b>5878</b>	<b>6069</b>

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
990	468	2	0	520

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	598	10	608
16 to 30 days	208	19	227
31 to 60 days	73	10	83
61 to 120 days	36	2	38
121 to 180 days	23	5	28
181 to 365 days	4	2	6
More than 365 days	0	0	0
<b>Total</b>	<b>942</b>	<b>48</b>	<b>990</b>

2.7 Requests for translation

Translation Requests	Accepted	Refused	Total
English to French	1	0	1
French to English	1	0	1
<b>Total</b>	<b>2</b>	<b>0</b>	<b>2</b>

**PART 3 – Disclosures under subsection 8(2)**

Paragraph 8(2)(e)	Paragraph 8(2)(m)	Total
0	0	0

**PART 4 – Requests for correction of personal information and notations**

	Number
Requests for correction received	3
Requests for correction accepted	1
Requests for correction refused	1
Notations attached	1

**PART 5 – Extensions**

5.1 Reasons for extensions and disposition of requests

Disposition of requests where an extension was taken	15(a)(i) Interference with operations	15(a)(ii) Consultation		15(b) Translation or conversion
		Section 70	Other	
All disclosed	35	0	0	0
Disclosed in part	121	0	6	1
All exempted	0	0	0	0
All excluded	0	0	0	0
No records exist	2	0	0	0
Request abandoned	1	0	0	0
<b>Total</b>	<b>159</b>	<b>0</b>	<b>6</b>	<b>1</b>

5.2 Length of extensions

Length of extensions	15(a)(i) Interference with operations	15(a)(ii) Consultation		15(b) Translation purposes
		Section 70	Other	
1 to 15 days	5	0	0	0
16 to 30 days	154	0	6	1
<b>Total</b>	<b>159</b>	<b>0</b>	<b>6</b>	<b>1</b>

**PART 6 – Consultations received from other institutions and organizations**

**6.1 Consultations received from other government institutions and organizations**

Consultations	Other government institutions	Number of pages to review	Other organizations	Number of pages to review
Received during the reporting period	17	270	3	490
Outstanding from the previous reporting period	0	0	0	0
<b>Total</b>	17	270	3	490
Closed during the reporting period	17	270	3	490
Pending at the end of the reporting period	0	0	0	0

**6.2 Recommendations and completion time for consultations received from other government 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	than 365 days	
Disclose entirely	5	0	0	0	0	0	0	5
Disclose in part	7	0	0	0	0	0	0	7
Exempt entirely	1	0	0	0	0	0	0	1
Exclude entirely	0	0	0	0	0	0	0	0
Consult other institution	0	0	0	0	0	0	0	0
Other	3	0	0	0	1	0	0	4
<b>Total</b>	16	0	0	0	1	0	0	17

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

Recommendation	Number of days required to complete consultation requests							Total
	1 to 15 days	16 to 30 days	31 to 60 days	61 to 120 days	121 to 180 days	181 to 365 days	than 365 days	
Disclose entirely	0	0	0	0	0	0	0	0
Disclose in part	0	0	0	0	1	1	0	2
Exempt entirely	0	0	0	0	0	0	0	0
Exclude entirely	0	0	0	0	0	0	0	0
Consult other institution	0	0	0	0	0	0	0	0
Other	1	0	0	0	0	0	0	1
<b>Total</b>	1	0	0	0	1	1	0	3

**PART 7 – Completion time of consultations on Cabinet confidences**

Number of days	Number of responses received	Number of responses received past deadline
1 to 15	0	0
16 to 30	0	0
31 to 60	0	0
61 to 120	0	0
121 to 180	0	0
181 to 365	0	0
More than 365	0	0
<b>Total</b>	<b>0</b>	<b>0</b>

**PART 8 – Resources related to the *Privacy Act***

**8.1 Costs**

Expenditures		Amount
Salaries		\$3,845,000
Overtime		\$59,000
Goods and Services		\$111,000
- Contracts for privacy impact assessments	\$0	
- Professional services contracts	\$6,000	
- Other	\$105,000	
<b>Total</b>		<b>\$4,015,000</b>

**8.2 Human Resources**

Resources	Dedicated full-time	Dedicated part-time	Total
Full-time employees	20.50	7.50	28.00
Part-time and casual employees	0.00	0.00	0.00
Regional staff	28.80	3.50	32.30
Consultants and agency personnel	0.01	0.01	0.02
Students	0.00	0.00	0.00
<b>Total</b>	<b>49.31</b>	<b>11.01</b>	<b>60.32</b>

**Additional Reporting Requirements – *Privacy Act***

Completed Privacy Impact Assessments (PIAs)

<b>Institution</b>	<b>Number of Completed PIAs*</b>
Human Resources and Skills Development Canada	6

\*A Privacy Impact Assessment (PIA) is not considered to be completed until the final, approved copy, has been sent to both the Office of the Privacy Commissioner and to the Information and Privacy Policy Division, Treasury Board of Canada Secretariat.