Annual Report on the Administration of the *Privacy Act*

2014-15

Employment and Social Development Canada

CA-600-03-16E

Canada

Annual Report on the Administration of the Privacy Act 2014-15

You can download this publication by going online: publicentre.esdc.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.

PDF
Cat. No.: Em1-5/2E-PDF
ISSN: 2369-0593

ESDC
Cat. No. : CA-600-03-16E

Table of Contents

Table of Figures

Executive Summary

Employment and Social Development Canada (ESDC) is responsible for a range of programs and services that support Canadians throughout their lives—from school to work, from one job to another, from unemployment to employment and from the workforce to retirement.

The mission of ESDC, which includes the Labour Program and Service Canada, is to build a stronger, more competitive Canada, support Canadians in making choices that help them live productive and rewarding lives, and improve Canadians' quality of life. It delivers programs and services directly to Canadians at over 600 points of service across Canada. ESDC serves the needs of millions of Canadians through multi-channel access points such as in-person services, on the Internet through web-based services and information, and via telephone through its network of call centres.

The protection of personal information is a core organizational value and is fundamental to maintaining the public's trust. The management and delivery of ESDC's programs and services often requires the collection, use, and disclosure of an individual's personal information. For some departmental programs, detailed and sometimes sensitive personal information is required to determine program eligibility or to receive benefits and services.

ESDC is subject to the personal information protection requirements set out in the *Privacy Act* as well personal information protection provisions in Part 4 of the *Department of Employment and Social Development Act*. Part 4 of the *Department of Employment and Social Development Act* imposes standards for the management and protection of personal information that take precedence over the requirements of the *Privacy Act*.

Privacy protection remains a key management priority at ESDC. In 2014-15, ESDC continued to make important progress on the implementation of its privacy management priorities. Key accomplishments include:

- strengthened planning and reporting on privacy through the establishment of an annual privacy and information security workplan;
- management and coordination of a significant volume of Privacy Impact Assessments on new programs and activities and continued modernization of the Privacy Impact Assessment process;
- updates to the departmental privacy policy suite, including the development of a new Directive on Privacy Impact Assessments and updated guidance on security incidents involving personal information (privacy breaches);
- continued implementation, review, and refresh of the Department's Program-Led Privacy Action Plans;
- review of the inventory of information sharing arrangements and initiation of an Information Sharing Arrangement risk triage exercise;
- privacy and security awareness activities for employees, including a Privacy Awareness Week and Data Privacy Day; and

- completed mandatory online privacy training for 13,800 employees as part of the *Stewardship of Information and Effective Workplace Behaviours* training module and 1,356 employees completed the online training module entitled *Privacy and Access to Information – Its Everyone's Business*.

Moving forward, the Department will continue in its efforts to promote a proactive, risk-based approach to privacy management and nurture an organizational culture committed to the stewardship of information.

1: Introduction

1.1: About the *Privacy Act*

The *Privacy Act* received Royal Assent on July 1, 1983. Its purpose is to impose obligations on federal institutions subject to the *Privacy Act* to respect the privacy rights of individuals by limiting the collection, use, and disclosure of personal information. The *Privacy Act* also gives individuals the right of access to their personal information and the right to request the correction of that information.

1.2: Section 72 Requirement in the *Privacy Act* to Report

Section 72 requires the head of a federal institution to submit an annual report to Parliament on the administration of the *Privacy Act* following the close of each fiscal year.

1.3: About Employment and Social Development Canada

The mission of Employment and Social Development Canada (ESDC), including the Labour Program and Service Canada, 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.

ESDC is one of the largest, distributed and complex federal departments in the Government of Canada. Citizens and clients interact with ESDC on a daily basis through over 600 points of service across Canada. Each year, ESDC provides support to millions of Canadians. In 2014-15, this included:

- 81.5 million visits to the Service Canada website;
- 8.1 million in-person visits to Service Canada centres;
- 1.9 million calls answered by 1 800 O-Canada agents;
- 4.7 million passports issued;
- 2.78 million Employment Insurance claims, 1.3 million Canada Pension Plan and 2.6 million Old Age Security and Guaranteed Income Supplement applications processed;
- $2.74 billion withdrawn from Registered Education Savings Plans by students to help fund their post-secondary education; and
- 94% of labour disputes settled as part of the collective bargaining process.

ESDC delivers a range of programs and services that affect Canadians throughout their lives. The Department provides seniors with basic income security, supports unemployed workers, helps students finance their post-secondary education and assists parents who are raising young children. The Labour Program is responsible for labour laws and policies in federally regulated workplaces. Service Canada helps citizens access ESDC's programs, as well as other Government of Canada programs and services.

To do this, ESDC:

- develops policies that make Canada a society in which all can use their talents, skills and resources to participate in learning, work and their community;
- creates programs and supports initiatives that help Canadians move through life's transitions—from families with children to seniors, from school to work, from one job to another, from unemployment to employment, and from the workforce to retirement;
- creates better outcomes for Canadians through service excellence with Service Canada and other partners; and
- engages its employees, establishes a healthy work environment, nurtures a culture of teamwork, and builds its leadership capacity.

In delivering on its mission, ESDC oversaw a budget of more than $112 billion in 2014-15.

1.4: About the Minister

The Honourable Pierre Poilievre was appointed Minister of Employment and Social Development, Minister for Democratic Reform and Minister responsible for the National Capital Commission in February 2015. He replaced the Honourable Jason Kenney, who became the Minister of National Defence and Minister for Multiculturalism.

2: Privacy Management at ESDC

ESDC is broadly recognized as holding more personal information than any other department in the Government of Canada. 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 distributed across branches and regions.

2.1: Legal Framework for Privacy

The *Privacy Act* protects the privacy of individuals with respect to their personal information held by government institutions. The *Privacy Act* also provides individuals with a right of access to that information as well as the right to request the 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*, the management of personal information at ESDC is also governed by Part 4 of the *Department of Employment and Social Development Act* which applies to the protection of personal information. Part 4 of the *Department of Employment and Social Development Act* establishes the rules that apply to the protection, use and making available of personal information obtained and prepared by ESDC. It contains privacy protection provisions which take precedence over those found in subsection 8(2) of the *Privacy Act* governing the disclosure of personal information.

2.2: Privacy Delegation

Section 73 of the *Privacy Act* and section 11 of the *Department of Employment and Social Development 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.

The Delegation Order**,** found in Annex A, outlines the delegations that were in effect throughout the 2014-15 fiscal year.

2.3: Departmental Privacy Management Framework

Given the importance of personal information protection at ESDC, the Department has adopted, and continues to implement, a risk-based and proactive approach to privacy management that promotes the concept of "privacy by design". Privacy by design emphasizes the importance of building privacy directly into the design and architecture of new programs, systems, technologies and business processes. ESDC's Privacy Management Framework includes the following key elements:

- **Element 1 – Governance and Accountability:** Roles and responsibilities for privacy management are clearly defined to meet legal requirements, regulations, policies, standards and public expectations.

- **Element 2 – Stewardship of Personal Information**: Appropriate privacy protections are implemented to manage personal information through its life cycle.

- **Element 3 – Assurance of Compliance**: Formal processes and practices are established to ensure adherence to privacy specifications, policies, standards and laws.

- **Element 4 – Effective Risk Management**: Structured and coordinated risk assessments are conducted to limit the probability and impact of negative events and maximize opportunities through risk identification, assessment and prioritization.

- **Element 5 – Culture, Training, and Awareness**: The protection of personal information is a core organizational value and is fundamental to maintaining the public's trust. Formal privacy training and awareness activities promote a privacy-aware organization that values the stewardship of information.

2.4: Privacy Governance

ESDC fosters governance and decision-making responsibilities for privacy through the Department's Corporate Management Committee, the Privacy and Information Security Committee, and associated sub-committees and working groups.

2.4.1: Corporate Management Committee

The Corporate Management Committee, a standing committee of ESDC's Portfolio Management Board, oversees the implementation of the portfolio's management agenda, as approved by the Portfolio Management Board, including the achievement of the management outcomes and objectives set out in the Integrated Business Plan, the Management Accountability Framework, and the corporate fiscal and planning processes. It also oversees departmental activities related to the operationalization of security and privacy plans and priorities.

2.4.2: Privacy and Information Security Committee

The Privacy and Information Security Committee, as a sub-committee of the Corporate Management Committee, reviews matters related to privacy and to the protection of personal information. The Privacy and Information Security Committee is co-chaired by the Chief Privacy Officer and the Departmental Security Officer.

The mandate of the Privacy and Information Security Committee is to:

- support the horizontal coordination and prioritization of issues, plans, and strategies related to the management and protection of personal information;

- review and provide advice to the Corporate Management Committee on the annual privacy and security work plan related to the protection of personal information, specific project terms of reference and project results;

- oversee the development, implementation and streamlining of key policies and processes to ensure privacy and security of personal information risks within the Department are mitigated;

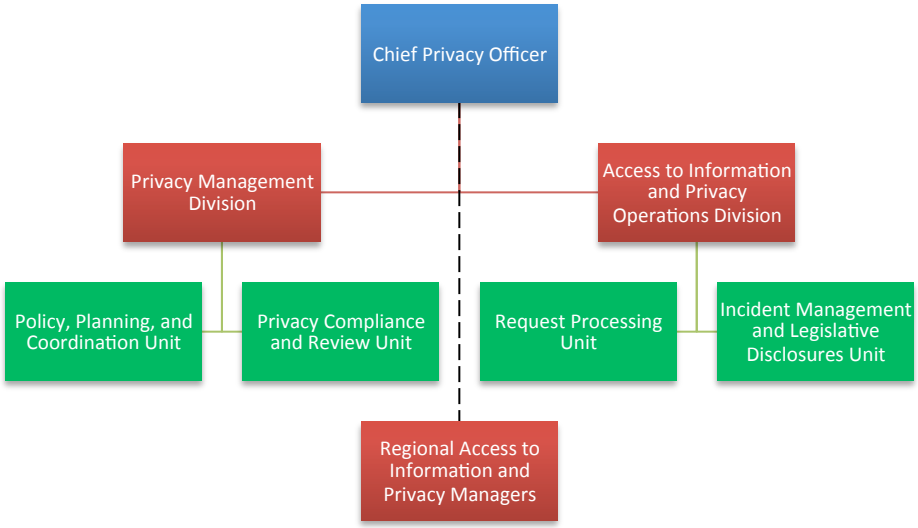
- review and provide advice to the Deputy Minister on privacy impact assessments and on information sharing agreements involving personal information;
- review and provide advice to the Corporate Management Committee on the portfolio-wide implications of significant privacy and personal information protection-related initiatives (e.g., Treasury Board Secretariat policies and directives, Management Accountability Framework assessments, audits and recommendations by the Office of the Privacy Commissioner, and federal-provincial tables on privacy and personal information sharing); 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).

2.4.3: Databank Review Working Group

The Privacy and Information Security Committee is supported by the Databank Review Working Group. It supports the application of privacy policy and the use of personal information for non-administrative purposes, including policy analysis, research and evaluation activities. The working group supports the development and review of projects that request the use of identifiable personal information and/or the linkage of personal information across databanks for such purposes.

2.5: Organization of the Privacy Function

Figure 1 – Organization of the Privacy Function at ESDC



The Corporate Secretariat is the Department's office of primary interest for the development of privacy policy, the provision of privacy advice and guidance to the portfolio, and the management of access to information and privacy operations. ESDC's Corporate Secretary serves as the Department's Chief Privacy Officer.

2.5.1: Chief Privacy Officer

The Chief Privacy Officer is the Department's functional authority on privacy matters, which includes the provision of authoritative advice and functional direction to all departmental branches and regions. The Chief Privacy Officer is responsible for the proactive management of privacy issues in the Department and the establishment of comprehensive privacy management frameworks, programs, review processes, and risk-based approaches to privacy management.

In addition to establishing departmental privacy directives, standards, guidelines, and processes, the Chief Privacy Officer is accountable for the implementation of the Department's privacy management program, including the coordination and management of privacy activities, which includes oversight of the Department's privacy governance structure with clear accountabilities and defined objectives that are aligned with departmental and government-wide policies, priorities and plans.

2.5.2: Privacy Management Division

The Privacy Management Division is the departmental focal-point for the management of privacy policy and the implementation of the Department's Privacy Management Framework. Under the authority and direction of the Chief Privacy Officer, the Privacy Management Division supports the horizontal coordination and implementation of departmental strategic plans and priorities as it relates to the protection of privacy, including the Department's multi-year Privacy Renewal Action Plan. The Division also manages the Department's privacy risk management function, including the privacy impact assessment process and the development of information sharing agreements involving personal information. The Privacy Management Division includes two units:

- The **Privacy Compliance and Review Unit** which provides advice, guidance, and privacy-related services to departmental officials on the application of relevant privacy legislation, policies, directives and guidance. This includes the management of the Department's Personal Information Banks in *Info Source*, the review of privacy notice statements, contracts, and other forms and instruments for privacy compliance, and the provision of advice and guidance for the development of information sharing agreements. The Unit is also tasked with day-to-day policy issues management related to the protection of personal information under the custody and control of the Department.

- The **Policy, Planning, and Coordination Unit** which is responsible for the development and implementation of the Department's privacy policy suite, strategic support services to the Chief Privacy Officer and the Privacy and Information Security Committee, and strategic planning and reporting functions. The Unit is also responsible for the design and implementation of the Department's Privacy Program, the privacy risk management process, the review and assessment of strategic policy and program priorities, and research and evaluation of emerging trends. The Unit also supports the management and implementation of horizontal issues and working groups.

2.5.3: Access to Information and Privacy Operations Division

The Access to Information and Privacy Operations Division carries out the Department's legislated requirements under the *Access to Information Act* and the *Privacy Act* by processing requests for access to records in the control of ESDC. The Access to Information and Privacy Operations Division coordinates

and advises on the processing of all requests under the *Access to Information Act* and is supported by program Liaison Officers and Regional Access to Information and Privacy Managers. The responsibility for processing *Privacy Act* requests is divided between the Access to Information and Privacy Operations Division and Regional Access to Information and Privacy Managers. This work involves responding to requests from the public and delivering training and awareness programs to employees with respect to administration of the two Acts. The Division is responsible for providing guidance to the regions with respect to the operational and reporting components of the access to information and privacy function.

In addition to its functions under the *Access to Information Act* and the *Privacy Act*, the Access to Information and Privacy Operations Division has delegated authority under the *Department of Employment and Social Development Act* to respond to legal instruments purporting to compel the disclosure of personal information, (i.e., subpoenas, production orders, search warrants) and to determine when to disclose personal information to third parties in the public interest.

The Access to Information and Privacy Operations Division also liaises with the Office of the Information Commissioner and the Office of the Privacy Commissioner regarding complaints received against the Department, and serves as the departmental point of contact with the Office of the Privacy Commissioner on privacy breaches.

The Access to Information and Privacy Operations Division includes two units:

- The **Request Processing Unit** performs a line-by-line review of records requested under the *Access to Information Act* and the *Privacy Act*. The Request Processing Unit provides weekly reports for information purposes to the Deputy Ministers' and Ministers' Offices on both new *Access to Information Act* requests and on upcoming *Access to Information Act* releases.

- The **Incident Management and Legislative Disclosures Unit (IMLDU)** determines when incidents involving personal information constitute privacy breaches and responds to legal instruments received by ESDC. The IMLDU also manages ESDC's response to complaints made to the Office of the Privacy Commissioner and interacts with the Office of the Privacy Commissioner on privacy breaches, working in partnership with the Departmental Security Office.

2.5.4: Regional Access to Information and Privacy Managers

While the Access to Information and Privacy Operations Director, with support from the Access to Information and Privacy Operations Division officers, has overall authority for the administration of the *Access to Information Act*, branches and regions also play a key role.

The Department has a network of Liaison Officers in the branches as well as Regional Access to Information and Privacy Managers who facilitate the work by providing expert *Access to Information Act* and *Privacy Act* advice and guidance directly to program areas in consultation with the Access to Information and Privacy Operations Division. The Liaison Officers also play a liaison role between Access to Information and Privacy Operations analysts and subject matter experts.

3: Privacy Activities and Accomplishments 2014-15

Privacy protection was a key management priority at ESDC in 2014-15. The Department continued to make important progress on the implementation of its privacy priorities to promote a proactive, risk-based approach to privacy management and to nurture an organizational culture committed to the stewardship of information. Accomplishments in 2014-15 include enhanced strategic planning to support privacy and security, privacy risk assessments of Departmental priority projects, and continued emphasis on privacy awareness and training activities. Highlights of key ESDC privacy activities and accomplishments are detailed below and which are organized by the elements of the Department's Privacy Management Framework.

3.1: Privacy Management Framework Element 1 – Governance and Accountability

3.1.1: Annual Privacy and Security Workplan (Privacy and Information Security Committee Priorities)

In 2014-15, the Department developed and implemented its annual integrated privacy and security workplan to support the strategic planning and implementation of the Department's privacy and security priorities. Overseen by the Privacy and Information Security Committee, the annual privacy and security workplan includes strategic and operational plans to achieve privacy and security management objectives, including a Privacy Management Action Plan. The 2014-15 Privacy Management Action plan shifted emphasis from the previous focus on renewal of privacy management functions to ongoing management and implementation of the Department's privacy program.

3.2: Privacy Management Framework Element 2 – Stewardship of Information

3.2.1: Department of Employment and Social Development Directive on Privacy Impact Assessments

In 2014-15, ESDC developed a new Directive on Privacy Impact Assessments. This Directive, which supports the Departmental Policy on Privacy Management, sets out ESDC's requirements, objectives, and expected results for privacy impact assessments and articulates the Department's responsibilities for ensuring that privacy implications will be appropriately identified, assessed and addressed when a new or substantially modified program or activity involving personal information is implemented. The Directive, and changes to the privacy impact assessment process, will come into force in 2015-16.

3.2.2: Departmental Directive on How to Respond to Security Incidents Involving Personal Information (Privacy Breaches)

In 2014-15, the Department updated its Departmental Directive on How to Respond to Security Incidents Involving Personal Information (Privacy Breaches). A security incident involving personal information is any act, event or omission that could result in the compromise of personal information. These potential privacy breaches may be the result of inadvertent or negligent errors or malicious

actions by employees, third parties, partners in information sharing agreements or intruders. Once it is determined that personal information has in fact been compromised, the potential security incident is referred to as a privacy breach.

The updated Directive provides ESDC employees and managers with information on their roles and responsibilities regarding the management of potential security incidents involving personal information. ESDC developed overarching Security Incident Reporting Protocols for the consistent management of all security incidents within the Department.

3.2.3: Program-Led Privacy Action Plans

In 2011-12, as part of the first phase of departmental privacy renewal activities, the Department conducted privacy risk assessments of eight of the Department's major programs to inform the prioritization of departmental privacy action plans. In 2012-13, ESDC developed Program-led Privacy Action Plans to mitigate potential privacy risks within the eight major programs. Implementation of the Program-led Privacy Action Plans continued in 2013-14, including bi-annual status reports on progress and results achieved to the Privacy and Information Security Committee.

In 2014-15, to facilitate the update of the Program-Led Privacy Action Plans, working groups were convened to coordinate branch efforts on risk assessment, workplan development, implementation, and reporting of progress. The privacy risk methodology, built upon the model used in 2011, was updated to incorporate lessons learned. A series of workshops were held with corporate enablers and program leads to discuss the strategy and roadmap for the next generation of refreshed action plans. In addition, a new approach for programmatic "action plan" development was established to improve compliance, including clear accountabilities for action plan elements as well as a common framework to collect foundational information to assess privacy risk and demonstrate compliance. Refreshed Program-Led Privacy Action Plans will be implemented 2015-16.

3.2.4: *Info Source* Update

In 2014–15, ESDC conducted a comprehensive review of its *Info Source* holdings. *Info Source* is a series of publications containing information about the Government of Canada's access to information and privacy programs. The primary purpose of *Info Source* is to assist individuals in exercising their rights under the *Access to Information Act* and the *Privacy Act*. *Info Source* also supports the government's commitment to facilitate access to information regarding its activities. As part of the review, ESDC created or updated 25 Personal Information Bank descriptions and over 30 Class of Records.

3.3 Privacy Management Framework Element 3 – Assurance of Compliance

3.3.1: Internal Audits on Privacy

As part of the implementation of ESDC's Privacy Management Framework, the Department has included select privacy-related internal audits and engagements in its internal audit plan. In May 2014, ESDC released its Audit of Program-Led Privacy Action Plans. The objective of the audit was to provide assurance that the Program-Led Privacy Action Plans were progressing or implemented as reported in the latest available updates. The audit identified findings and recommendations with respect to the development and implementation of refreshed action plans, ongoing monitoring of the plans, and

reporting on the plans. Senior management accepted the recommendations and actions commenced with the major departmental programs to implement the internal audit findings.

3.3.2: Follow-up on Security Incidents Involving the Loss of Portable Storage Devices

The 2012-13 Annual Report to Parliament on the Administration of the *Privacy Act* reported on two incidents involving the loss of personal information. During the 2014-15 reporting period, ESDC continued the implementation of its USB Storage Devices Directive which restricts the use of portable storage devices to instances where management has validated the need, mandates the use of encrypted USB keys or hard drives, and imposes consequences for failure to comply. ESDC continued to monitor desktop computers for unauthorized USB devices and deployed security software to block all other portable storage devices, such as optical media (CD/DVD) and floppy disks. Only authorized users can save to such media.

In addition, ESDC continued regular security sweeps in its buildings including employee workstations. This measure was intended to raise awareness with employees while simultaneously mitigating potential privacy incidents. ESDC also continued to execute its information management strategy across all branches and regions.

3.3.3: Office of the Privacy Commissioner Investigation into the Loss of a Hard Drive at ESDC

On March 25, 2014, the Office of the Privacy Commissioner released its findings on the investigation of the loss of a portable hard drive containing the personal information of 583,000 Canada Student Loan beneficiaries. The Special Report to Parliament from the Office of the Privacy Commissioner contained 10 recommendations. The investigation noted that ESDC accepted all of the recommendations from the Office of the Privacy Commissioner in full and that ESDC was well-advanced in the implementation of many of the recommendations identified. The report also stated that the Office of the Privacy Commissioner was satisfied that no further action is required by its office at that time, and that the Office of the Privacy Commissioner will follow-up with ESDC in one year to confirm the Department's progress in the implementation of recommendations. In 2014-15, ESDC provided to the Office of the Privacy Commissi9oner a final update on ESDC's implementation of the recommendations made in the 2014 Records of Finding. The OPC's investigation is now closed.

3.4 Privacy Management Framework Element 4 – Effective Risk Management

3.4.1: Implementation of the Redesigned Privacy Impact Assessment Process

In 2012-13, ESDC initiated a project to re-design its privacy impact assessment process, including the piloting of a structured and coordinated privacy risk assessment process, the standardization and streamlining of its privacy impact assessment reports, and the early identification and triage of privacy impact assessments. In addition to a 66% increase in the number of privacy impact assessments approved in 2013-14, the Department significantly increased the number of privacy impact assessments under development.

In 2014-15, ESDC continued to prioritize improvements to build and mature its privacy impact assessment process and privacy and security risk assessment activities. Seven privacy impact assessments were completed in 2014-15, based on the Treasury Board Secretariat definition of a completed privacy impact assessment; however, a significant volume of privacy impact assessments were also in various stages of development and required sustained attention.

3.4.2: Implementation of an Information Sharing Arrangements Workplan

In 2014-15, the Department continued the implementation of its Information Sharing Arrangement Workplan. Progress was made on elements of the workplan which included: an update of the Department's list of arrangements; collaboration with departmental stakeholders to develop a methodology to triage arrangements based on potential risk to personal information; creation of an electronic inventory and online RAPID Triage Questionnaire to help identify potential risks to respective arrangements; engagement of responsible branches and regions to review existing arrangements; and the initiation of a preliminary analysis of information sharing arrangement data to identify trends and provide information on potential indicators of risk.

3.5 Privacy Management Framework Element 5 – Culture, Awareness and Training

3.5.1: Raising Privacy Awareness

The Department continued to promote practical, easy to understand, readily available information and guidance to employees to reinforce proper privacy protection practices throughout 2014-15. The Department continued to update an internal Stewardship of Information web site available to employees. The web site is a repository of information on the related themes of privacy, information management, physical, personnel, and information security, information technology security, and values and ethics. Each theme highlights information on employee roles and responsibilities, relevant policies and guidance, frequently asked questions, links to mandatory training, and contact information. The site also hosts a video introducing the concept of information stewardship, which was promoted extensively throughout the year in corporate communications and on corporate web sites.

ESDC convened a Privacy Awareness Week from May 4 to May 10, 2014, and on January 28, 2015, ESDC celebrated Data Privacy Day. Corporate messages were sent to all employees to raise awareness of their roles and responsibilities for the protection of personal information.

3.5.2: Online Privacy Training to enhance Stewardship of Information

The Department continued to provide a mandatory training module on the Stewardship of Information and Effective Workplace Behaviours. The mandatory integrated module covers six disciplines related to the stewardship of information (security, information management, information technology security, values and ethics, privacy, and access to information). New to employees in 2013-14, this course continues to support the Department's commitment to ensuring the responsible use and care of departmental and personal information. In 2014-15, 13,800 employees completed the *Stewardship of Information and Effective Workplace Behaviours* course. In addition, the Department has established an online training module entitled *Privacy and Access to Information – It's Everybody's Business*. In 2014-15, 1,356 employees had completed the module.

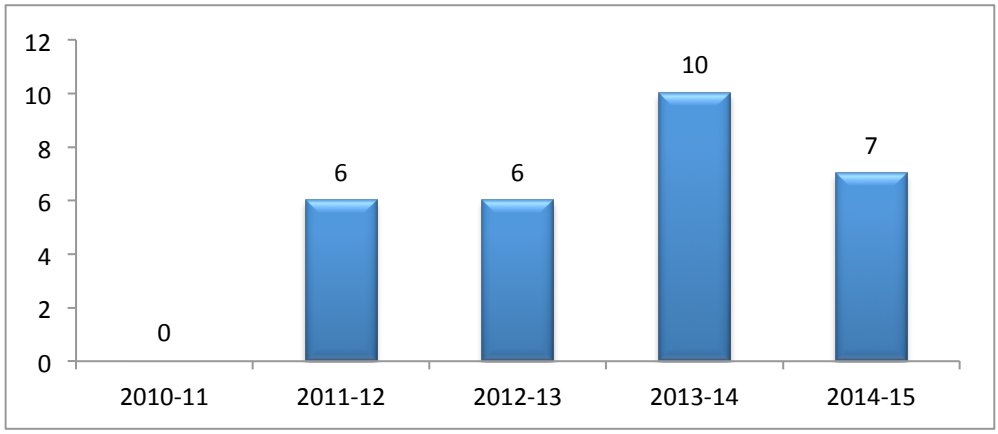
4: Privacy Performance Reporting for 2014-15

Figure 2 – Requests Received and Completed Under the *Privacy Act*

Activity	2010-11	2011-12	2012-13	2013-14	2014-15
Completed Privacy Impact Assessments Forwarded to the Office of the Privacy Commissioner	0	6	6	10	7
Formal Requests Received Under the *Privacy Act*	12,136	10,737	7,639	7,286	7,998
Requests Completed During the Reporting Period	12,010	10,830	7,493	7,239	7,781
Requests Completed Within 30 Calendar Days	10,179	9,944	6,315	6,727	6,983
Requests Completed Within 31 to 60 Calendar Days	1,776	732	1,002	417	663
Requests Completed Within 61 or More Calendar Days	55	154	176	95	135
Disclosures in the Public Interest	35	78	7	206	211
Complaints to the Privacy Commissioner	17	24	17	27	18
Material Privacy Breaches	--	--	--	0	3

4.1: Completed Privacy Impact Assessments

Figure 3 – PIAs Forwarded to the Office of the Privacy Commissioner



Privacy impact assessments are policy processes for identifying, assessing and mitigating privacy risks. Government institutions are required to develop and maintain privacy impact assessments for all new or modified programs and activities that involve the use of personal information for an administrative purpose. According to the Treasury Board Secretariat, "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." According to this definition, ESDC completed seven privacy impact assessments in 2014–15.

Summaries of the seven privacy impact assessments completed in 2014-15 will be made available online on the departmental website.

4.1.1: Canada Apprentice Loan Phase I: Loan Set-Up and Processing

In Budget 2014, the Government of Canada announced the creation of the Canada Apprentice Loan (CAL) to assist registered apprentices with the cost of technical training. Under this initiative, apprentices registered in Red Seal trades will be able to apply for loans of up to $4,000 per period of block release technical training. These loans will help offset the cost to apprentices to complete these periods of technical training required by their program.

The CAL will be administered by the Canada Students Loans Program's (CSLP) current service provider. The program's web presence, online administration, contact centre and account management will operate separately from the CSLP. Personal information will be collected to support the administration of these loans and will be used to confirm program eligibility. Personal information will also be exchanged with other federal institutions, provincial/territorial jurisdictions, credit bureaus as well as technical training providers for the administration and delivery of the CAL.

A privacy impact assessment was performed to provide evidence of compliance with legislative requirements and to report to management on the privacy related risks that were identified and assessed related to the implementation of the CAL.

4.1.2: Enabling Services Renewal Program (ESRP) my EMS (PeopleSoft)

On May 1, 2012, Treasury Board Secretariat's Office of the Chief Human Resources Officer established a new standard for managing Human Resource transactions across the Government of Canada. The implementation of myEMS (PeopleSoft) is part of a Government of Canada initiative to replace the multiple HR systems and applications with one standard version.

On April 7, 2015, myEMS (PeopleSoft) will replace the Department's aging, custom-built human resources (HR) system – Corporate Management System and Paperless Office for the collection and management of employee information (e.g. classification, staffing, compensation, leave and training information). The Office of the Chief Human Resources Officer designed the data requirements (i.e. metadata) and ESDC collects and retains personal information (that matches the Office of the Chief Human Resources Officer metadata) in order to properly administer the management of employee information for HR purposes. MyEMS (PeopleSoft) will use the Government of Canada Pay Interface to send personal information related to pay transactions to the Government of Canada Regional Pay System.

A privacy impact assessment was performed to identify privacy impacts and risks associated with the implementation of myEMS (PeopleSoft), including current mitigations and a list of action items to further mitigate identified risks.

4.1.3: Job Bank 2.0 New Login Solution

Job Bank offers a free online job board that allows employers to post available job opportunities and allows job seekers to search for employment. In the 2014 Economic Action Plan, the Government of Canada committed to invest in an enhanced Job Match Service with a secure authentication process within Job Bank, including a new login solution. The login solution upgrades will include an enhanced authentication process to strengthen controls over account genuineness, granting access only to valid users who are either looking for work or looking to hire qualified job seekers.

The Job Bank service also supports the Citizenship and Immigration Canada (CIC)-led Express Entry (EE) program, which is designed to create a pool of employment-ready skilled workers to meet Canada's labour market needs. The EE represents a new and mandatory pre-application stage for certain prospective immigrants interested in specific permanent residence program streams in Canada. The role of ESDC in the EE initiative is to grant access to EE candidates to Job Bank and allow their job seeker profile to be matched with jobs based on their individual skills, education, credentials and experience.

Personal information will be used to authenticate the identity of Canadians and permanent residents while personal information from CIC`s EE system will be used to authenticate foreign nationals who are EE candidates. A Memorandum of Understanding between ESDC and CIC outlines the administrative framework for the exchange of EE data elements.

A privacy impact assessment was performed to identify privacy impacts and risks associated with the new Job Bank login solution (Job Bank 2.0), including current mitigations and a list of action items to further mitigate identified risks.

4.1.4: Provincial and Territorial Delivery of the Canada Job Grant

To help equip Canadians with the skills and training they need to fill available jobs, the Government of Canada is renewing and transforming the Labour Market Agreements with provinces and territories into new Canada Job Fund agreements, which include the Canada Job Grant (CJG).

The CJG is a cost-shared program designed to offset the direct costs of training Canadian employees (e.g. tuition and training materials) through the provision of grants of up to $10,000 per beneficiary to eligible employers who are training potential or existing employees for new or better jobs. The provinces and territories will be responsible for delivering the CJG in their respective jurisdictions. The provinces and territories will provide personal information to ESDC on employers receiving the CIG on a monthly basis. Only information from consenting employers will be shared. The information will be used by ESDC to identify and secure communications opportunities to promote the CJG.

A privacy impact assessment was performed to identify the privacy impacts and risks associated with the implementation of promotional activities for CJG, and provide recommendations for their resolution or mitigation.

4.1.5: Skills and Partnership Fund

In 2010, two programs that complement each other, the Aboriginal Skills and Employment Training Strategy (ASETS) and the Skills and Partnership Fund (SPF) were launched with the objective of increasing Aboriginal participation in the Canadian labour market. The SPF is a demand-driven, partnership-based contributions program which funds short-term projects supporting the skills development, training and employment of Aboriginal people. It consists of an investment of $210 million over five years (2010-11 to 2014-15).

The recent extension of the SPF for an additional year (2015-16) allows time to complete the design of renewed and enhanced programming for implementation in 2016-17, as well as the solicitation and review of project proposals. Personal information is collected directly by the agreement holders to administer the program, obtain views and opinions on the programs through a participant survey, conduct accountability activities such as monitoring and evaluation, and ensure data quality.

A privacy impact assessment was performed to identify privacy impacts and risks for the SPF. It also includes current mitigations and a list of action items to further address the identified risks.

4.1.6: Temporary Foreign Worker Program Phase II

The Temporary Foreign Worker Program (TFWP) assists employers in filling their genuine skill and labour requirements, on a temporary basis, when qualified Canadians and permanent residents are not available. It is an option of last resort for employers to address temporary and immediate labour shortages. ESDC/Service Canada evaluates employer applications and issues Labour Market Impact Assessments (LMIAs) based on the likely impact of hiring temporary foreign workers on the Canadian job market.

The privacy impact assessment for TFWP was divided into different phases to meet the tight timelines associated with the implementation of the numerous TFWP program changes. Phase I of the privacy impact assessment was approved in October 2013.

Phase II of the TFWP privacy impact assessment considered the privacy impacts of further changes to the LMIA application process, the handling of Social Insurance Numbers in client documents, employer plans to transition to a Canadian workforce, the Federal Skilled Workers/Federal Skill Trades Programs, and ministerial instructions. In addition, the Phase II PIA provided an update on the current status of the implementation of risk mitigation activities identified in Phase I.

4.1.7: Privacy Impact Assessment and Information Sharing Agreement between the Canada Border Services Agency and Employment and Social Development Canada for the Temporary Foreign Worker Program

The Temporary Foreign Worker Program (TFWP) allows employers to hire foreign workers as a last resort to meet their short-term labour and skills needs. The program is jointly managed by ESDC, Citizenship and Immigration Canada and the Canada Border Services Agency (CBSA), under the authority of the *Immigration and Refugee Protection Act* (IRPA) and the *Immigration and Refugee Protection Regulations*.

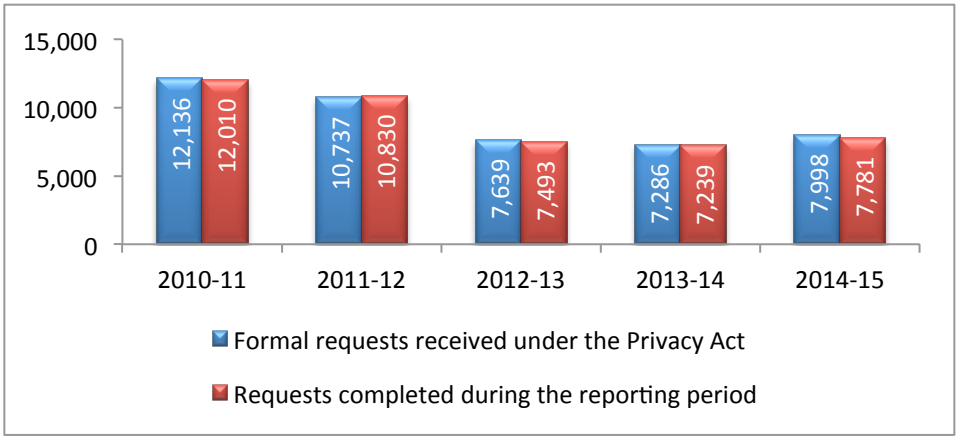
On June 20, 2014, the Minister of Employment and Social Development announced broad reforms to the TFWP to reduce employer use of, and reliance on, foreign nationals and ensure greater compliance with Program requirements. This included a commitment to establish new conditions for information sharing.

The March 11, 2015 amendments to the Department of Employment and Social Development Regulations provided ESDC with the authority to disclose personal information to the CBSA to further enable the Agency to fulfill its mandate for the administration and enforcement of IRPA. The purposes, modalities and protections in relation to the exchange of personal information between ESDC and the CBSA are set out in the Information Sharing Agreement.

A privacy impact assessment was performed to identify the privacy impacts and risks associated with the Information Sharing Agreement between ESDC and the CBSA.

4.2: Requests for Information Under the *Privacy Act*

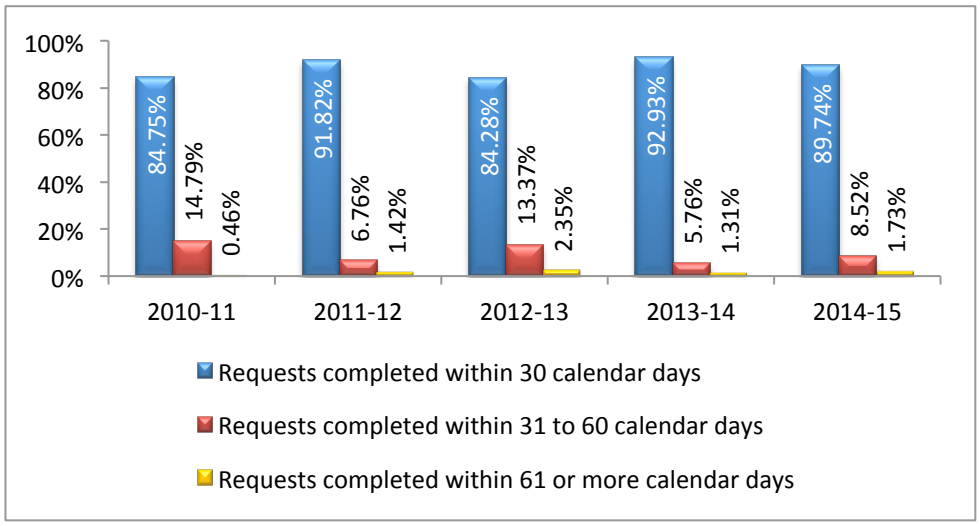
Figure 4 – Requests Received and Completed Under the *Privacy Act*



The current reporting period saw a slight increase in the number of requests received by ESDC following four consecutive years of decreases. During the same time frame, the difference between the number of requests received and the number of requests completed in a given fiscal year has been less than 1% on average. In 2014–15, ESDC received 7,998 requests under the *Privacy Act* and completed 7,781 requests. The number of requests completed may include requests received in a previous reporting period but completed in 2014-15. 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 federal employees seeking to obtain a copy of their personnel information.

4.3: Requests by Calendar Days Taken to Complete

Figure 5 – *Privacy Act* Requests by Calendar Days Taken to Complete as a Percentage of Total



The percentage of *Privacy Act* requests completed within 30 calendar days during the last five reporting periods remains on average nearly 89%.

4.4: Pages Reviewed

In 2014-15, a total of 633,787 pages were reviewed (processed). Of these, 603,090 pages, or 95%, were disclosed to the requester. Of the number of requests disclosed, 6,825 involved processing 500 pages or less, with 5.139 requests requiring the review of 100 pages or less and 1,686 requests requiring the review of between 101 and 500 pages.

4.5: 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 of 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." In 2014-15, consultations were required for 34 requests while 330 requests contained interwoven information. No requests required legal advice and 389 requests were classified as other.

4.6: Performance

In 2014-15, the Department was able to meet its legislated timeline over 95% of the time with only 4.1% of all requests outstanding during the reporting period. This is a slight improvement over the 4.5% of late files for 2013-14. Workload was the most common cause for not meeting a legislated timeline and was the cause of 208 files being disclosed late. Internal and external consultations accounted for 7 and 2 cases respectively while 25 timelines were not met for reasons listed as "other".

4.7: 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 to 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 2014-15, ESDC claimed an extension on 235 requests. This represents an increase from 2013-14 when the Department claimed extensions on 153 requests. Of the 235 extensions, 217 were based on interference with operations, 11 were for translation or conversion and 7 were for other reasons.

4.8: Translation of Records

In 2014-15, a total of 10 requests were made for the translation of records by applicants. One request was for translation from English to French, and nine were for translation from French to English. In all ten cases the records were translated as requested.

4.9: Requests for Correction of Information

Individuals have a right to request correction of any erroneous personal information pertaining to them providing that the individual can adequately substantiate the request. Six requests for correction of personal information were received in 2014–15. Three requests were accepted while the remaining three resulted in a notation being attached to the file.

4.10: Consultations Received From Other Institutions and Organizations

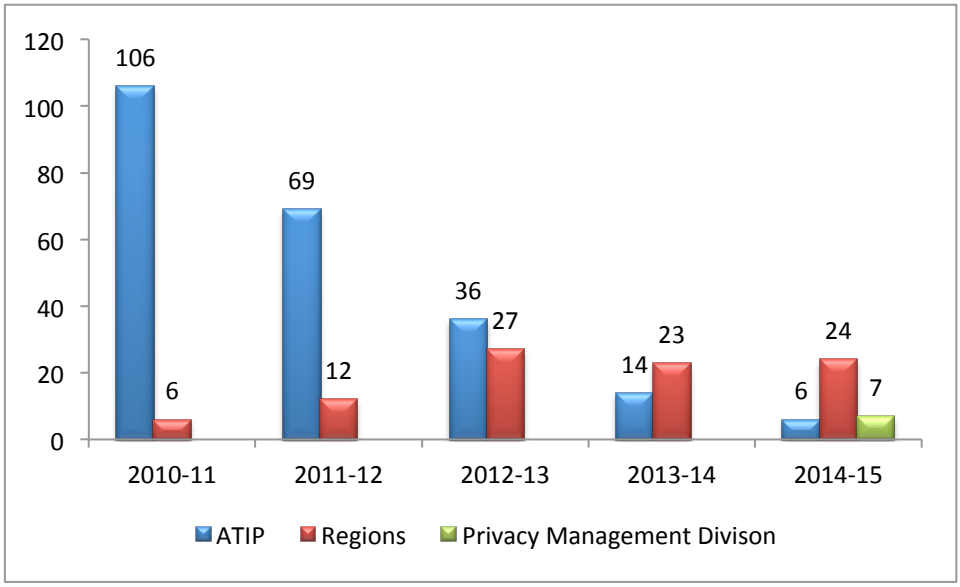
ESDC responded to 10 consultations in 2014–15, all of which were received from other government institutions, corresponding to a review of 199 pages. Eight of these consultations resulted in a recommendation to entirely disclose the records, two recommended that the consulting department or organization disclose in part. Consultations with ESDC Legal Services on Cabinet Confidences were not required during the reporting period.

4.11: Financial Considerations

In 2014–15, the Department spent $3.4 million on salaries associated with administering the *Privacy Act* as well as $65,631 on overtime. Non-salary costs amounted to $340,597 bringing total expenditures to $3.8 million. A total of 67.11 person years were dedicated to privacy activities. This figure can be further broken down to 34.65 person years for regional staff, 26.36 person years for National Headquarters staff, 3.34 person years for part-time and casual employees, 2.00 person year for consultants and agency personnel and 0.76 person years for students.

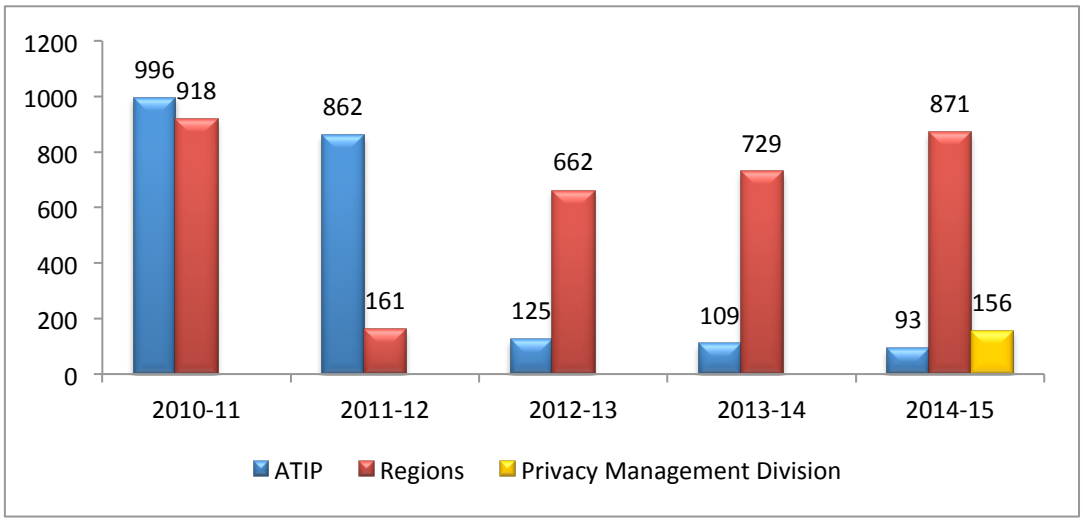
4.12: Privacy Training Activities

Figure 6 – In-Person Training Sessions Offered at National Headquarters and in Regional Offices



Note: Privacy Management Division began its first full fiscal year of operations in 2014-15.

Figure 7 – In-Person Employee Trained at National Headquarters and in Regional Offices



Note: Privacy Management Division began its first full fiscal year of operations in 2014-15.

Figures 6 and 7 provide statistical information on specific ATIP training delivered by the ATIP Operations Division over the past five years. This also includes specific privacy-related training delivered by the Privacy Management Division in 2014-15 – its first full fiscal year of operations.

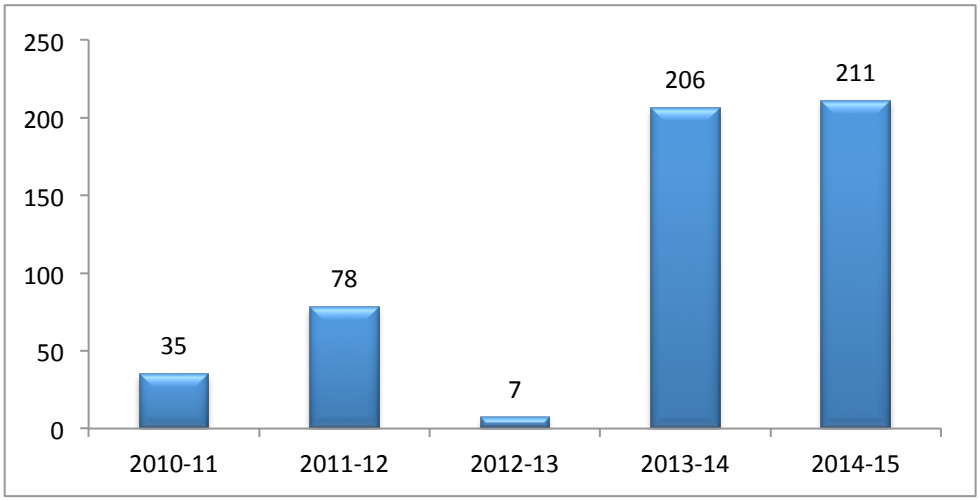
These figures do not reflect all privacy-related training completed by ESDC employees. For example, the Department released its mandatory online Stewardship of Information and Effective Workplace Behaviours training program in 2013-14 which included specific training modules on access to information and privacy. In 2014-15, 13,800 employees had completed the mandatory online training. In addition, 1,356 employees completed the online training module *Privacy and Access to Information – It's Everybody's Business* in 2014-15.

In 2014–15, the Access to Information and Privacy Operations Division provided six in-person training sessions on access to information and privacy issues to 93 employees across the Department. In response to recurring questions from program experts regarding the scoping of records and on the formulation of recommendations regarding the exemption and exclusion provisions of the *Access to Information Act*, the Access to Information and Privacy Operations Division updated and shared its guidance on these topics with program areas. Recognizing that not all employees are tasked with requests on a regular basis, the guidance is brief and provides key pointers to assist those responsible for gathering records to fulfill their responsibilities.

In 2014–15, the Privacy Management Division provided seven in-person training sessions on privacy issues to 156 employees across the Department. In response to internal stakeholder requests for specific privacy topics, information sessions or boot camps were held on how to develop and implement privacy impact assessments, information sharing arrangements and personal information banks. In addition, the Privacy Management Division provided regular advice and guidance on these and other privacy-related topics to support internal stakeholders in their roles and responsibilities in the safeguarding and protection of personal information within the custody and control of the Department.

4.13: Public Interest Disclosures Reported to the Office of the Privacy Commissioner

Figure 8 – Public Interest Disclosures Reported to the Office of the Privacy Commissioner



As per section 2.1, "ESDC's Legal Framework for Privacy" Part 4 of the *Department of Employment and Social Development Act* takes precedence over section 8(2) of the *Privacy Act* as it relates to the disclosure of personal information. Accordingly, any disclosures in the public interest are made in accordance with subsection 37(1) of the *Department of Employment and Social Development Act*, which states that personal information may be disclosed:

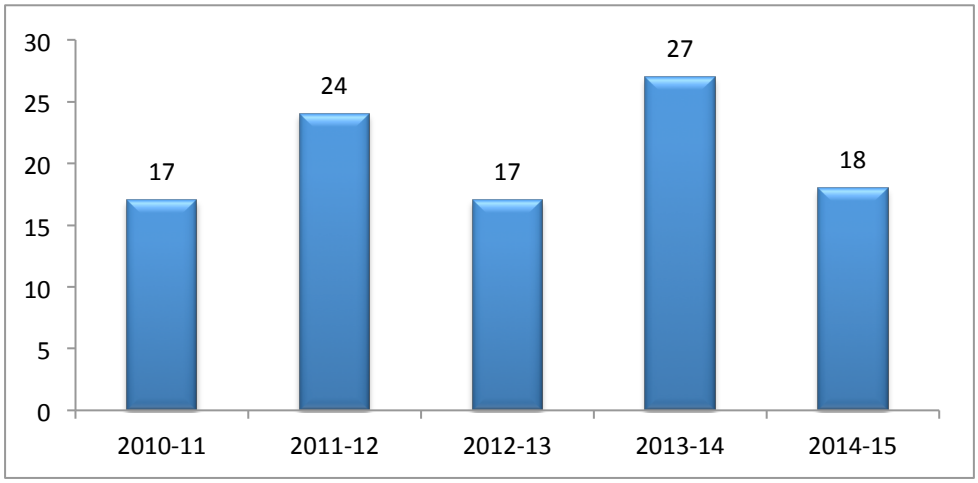
> *…if the Minister is of the opinion that the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure or that disclosure would clearly benefit the individual to whom the information relates.*

In 2013-14, 206 disclosures were recorded which included 114 public interest disclosures previously mentioned in 2012-13. These 114 disclosures should have been more accurately represented as having been completed in 2013-14 which is when they were reported to the Office of the Privacy Commissioner. Figure 8 portrays 7 disclosures as having been completed and reported in 2012-13.

In 2014-15 the Department notified the Office of the Privacy Commissioner of 211 public interest disclosures under subsection 37(1) of the *Department of Employment and Social Development Act*. In 48 files, the information was disclosed in the previous fiscal year but the Office of the Privacy Commissioner was notified in 2014-15.

4.14: Complaints and Investigations

Figure 9 – Complaints Received by the Office of the Privacy Commissioner



In 2014-15, the Department was notified of 18 complaints received by the Office of the Privacy Commissioner. Of these cases, 10 related to delay, two related to denied access, one pertained to improper disclosure, and five pertained to improper use and disclosure.

In the same fiscal year, ESDC received findings on a total of 14 complaints. The Office of the Privacy Commissioner ruled eight were well founded, one was not well founded, one was settled in the course of the investigation, and four were discontinued.

4.15: Material Privacy Breaches

ESDC reported three material breaches to the Office of the Privacy Commissioner in 2014-15.

Material Breach 1

On April 30, 2014, Service Canada misdirected a list of 147 individuals to an employer. The employer was to have been consulted on only one individual to confirm eligibility for Employment Insurance. Upon noting the error, the employer immediately contacted Service Canada to alert them to the fact that they had received the list in error. The Service Canada regional security office conducted a fact-finding exercise. The Regional Security Officer also contacted the employer. The employer confirmed that the data they received in error had been destroyed.

The Access to Information and Privacy Operations Division, the Security Incident Management Unit and the relevant region worked together to address the privacy breach. The personal information disclosed was name, Social Insurance Number, name of the employer, union affiliation, and industry. Letters were sent to the individuals affected.

To address the error there was a discussion with the individual responsible and the unit was sensitized to the need to review electronic communications carefully to prevent inadvertent disclosure.

Material Breach 2

On May 5, 2014, a Service Canada Old Age Security Mail Processing Centre misdirected proactive applications for Old Age Security allowance benefits of 98 individuals. Each application package contained an English and French personalized letter along with an English and French application. Service Canada became aware that, in the process of mailing the applications, an error occurred resulting in a client receiving their letter in one language and another individual's letter in the other language. The region was unable to determine whether it was a human or machine error.

The Access to Information and Privacy Operations Division, the Security Incident Management Unit and the relevant region worked together to address the privacy breach. The personal information disclosed was name, address and Social Insurance Number. Letters were sent to the individuals affected.

Follow-up processes included: the Team Leader notified the Citizen Services Business Expertise group and a general enquiry was sent to the Old Age Security Mail Processing Centre; the process was modified so that the employee scanning the letters was not the employee who scanned the documents (a second pair of eyes); and the application was sent in only one official language unless otherwise required.

Material Breach 3

On August 20, 2014, a briefcase containing 20 files relating to the New Horizons for Seniors program was stolen from an employee's vehicle in Montréal, Québec, while the employee attended a meeting. The theft was immediately reported to the Department and to the police.

The Access to Information and Privacy Operations Division, the Security Incident Management Unit and the relevant region worked together to address the privacy breach. Information contained in the documents included individuals' names, addresses, telephone numbers, nationality, date of birth, e-mail addresses and information about their professions. Each individual was impacted differently, depending on what personal information had been submitted to the Department. Given the time required to reconstruct the files, individuals were contacted between September 23 and 29, 2014. A total of 157 individuals were affected. Letters were sent to 98 individuals as contact information could not be confirmed for the remainder.

In response to this incident, employees were reminded of the procedures in place for transporting and storing Protected B information.

5: Moving Forward

Moving forward, the Department will continue in its efforts to promote a proactive, risk-based approach to privacy management and nurture an organizational culture committed to the stewardship of information. It will continue the implementation of the privacy program that supports the continuous improvement of controls and practices related to sensitive and personal information. The Department will also continue its awareness efforts to ensure that both employees and clients are aware of the threats or other attempts to gather personal information through various methods and techniques.

Annexes

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

Delegated Officials	Delegated Authority	*Department of Human Resources and Skills Development Act* provision (Repealed, 2012, c. 19, s. 685)	*Department of Social Development Act* provision (Repealed, 2012, c. 19, s. 685)
Deputy Minister, ESDC Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, Access to Information and Privacy (ATIP)	*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.*	33(2)	27(2)
Deputy Minister, ESDC	*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*	35(2)	29(2)
Deputy Minister, ESDC	*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*	35(3)	29(3)

Deputy Minister, ESDC	*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*	36(1)	30(1)
Deputy Minister, ESDC	*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.*	36(2)	30(2)
Deputy Minister, ESDC	*Determining whether it is advisable for a government, public body, organization or institution to which information was made available under subsection 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*	36(3)	30(3)
Deputy Minister, ESDC Senior Associate Deputy Minister/ Chief Operating Officer	*Determining whether the public interest in disclosing the information clearly outweighs any invasion of privacy that could result from the disclosure*	37(*1*)	31(*1*)

Associate Deputy Minister Corporate Secretary Director, ATIP **For only those situations where there is a threat to the safety and/or security of an individual:** departmental Security Officer Regional Security Officers Regional Privacy Coordinators Service Area Managers Call Centre Managers Manager, Corporate Security Security Advisor, Corporate Security	*or determining whether disclosure would clearly benefit the individual to whom the information relates.*		
Deputy Minister, ESDC Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP	*Authority to notify the Privacy Commissioner*	37(2)	31(2)
Deputy Minister, ESDC	*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.*	38(a)	32(a)
Deputy Minister, ESDC	*Determining whether the research or statistical purpose for which information is to be made available to any person or body cannot reasonably be*	38(b)	32(b)

	accomplished unless the information is provided in a form that may identify the individual to whom the information relates		
Deputy Minister, ESDC	*Determining the conditions under which the information may be made available for research or statistical purposes to any person or body*	38(c)	32(c)
Deputy Minister, ESDC Senior Assistant Deputy Minister Strategic Policy and Research	*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.*	39(2)	33(2)
CRIMINAL: Deputy Minister, ESDC Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP **CIVIL:** Deputy Minister, ESDC Senior Associate Deputy Minister/ Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP	*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*	40	34

ADM, Ontario Region Regional Executive Heads Regional Privacy Coordinators			

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

Delegated Officials	Delegated Authority	*Department of Human Resources and Skills Development Act provision*	*Department of Social Development Act provision*
Deputy Minister, HRSD	*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*	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	8(2)(m)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary

whom the information relates		Director, ATIP **For those situations where there is a threat to the safety and/or security of an individual:** departmental Security Officer Regional Security Officers Regional Privacy Coordinators Service Area Managers Call Centre Managers Manager, Corporate Security Security Advisor, Corporate Security
Retention of a record of requests and disclosed records to investigative bodies under section 8(2)(e) of the *Privacy Act*.	8(4)	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
Notification of the Privacy Commissioner of all disclosures made under paragraph 8(2)(m) of the *Privacy Act* (public interest).	8(5)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary

		Director, ATIP Managers, ATIP
Retention of records of uses of personal information	9(*1*)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP
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)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP
Include personal information in personal information banks	10(1)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP
Respond to request for access within 30 days and give written notice and, if access to be given, give access.	14	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 A1
Extension of the 30 day time limit to respond to a privacy request.	15	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 Public Rights Analyst, ATIP Regional Privacy Coordinators Positions as per Annex A1
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 A1
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 A1
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	19(1)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP

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.		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 Managers, ATIP Senior Public Rights Administrator, ATIP Regional Privacy Coordinators
Refuse to disclose information that may be injurious to the conduct of federal-provincial affairs	20	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP
Refuse to disclose information that may be injurious to international affairs or the defence of Canada or one of its allies.	21	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary

		Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP
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	22	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 A1
Refuse to disclose information prepared by an investigative body for security clearance.	23	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 that was collected by the Canadian Penitentiary Service, the National Parole Service or the National Parole Board	24	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer

while the individual was under sentence if the conditions in the section are met		Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Regional Privacy Coordinators
Refuse to disclose information which could threaten the safety of individuals	25	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP 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 A1
Refuse to disclose information that is subject to solicitor-	27	Deputy Minister

client privilege.		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 Corporate Secretary Director, ATIP Managers, ATIP Senior Public Rights Administrator, ATIP Regional Privacy Coordinators
Receive notice of investigation by the Privacy Commissioner	31	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP
Right to make representations to the Privacy Commissioner during an investigation	33(2)	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
Receive Privacy Commissioner's report of findings of an investigation and give notice of action taken	35(1)	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
Provision of addition information to a complainant after receiving a 35(1)(b) notice.	35(4)	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
Receive Privacy Commissioner's report of findings of investigation of exempt bank	36(3)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP
Receive report of Privacy Commissioner's findings after compliance investigation	37(3)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP
Request that a court hearing, undertaken with respect to certain sections of the Act, be held in the National Capital Region.	51(2)(b)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP Managers, ATIP
Request and be given right to make representations in section 51 hearings	51(3)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary

		Director, ATIP Managers, ATIP
Prepare annual report to Parliament	72(1)	Deputy Minister Senior Associate Deputy Minister/Chief Operating Officer Associate Deputy Minister Corporate Secretary Director, ATIP

Positions Delegated in the Regions, as Noted in the Delegation Instrument

Atlantic Region

No additional positions identified.

Québec Region

Title	Position number	Sections
Regional Office		
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

Title	Position number	Sections
Regional Office		
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 (bilingual)	14, 15, 17(2)(b), 17(3)(b), 22, 26, 27, 28
ATIP Officer	54688 (bilingual)	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

Title	Position number	Sections
Regional Offices		
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
Local Offices		
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 Officer	70255	14, 15, 17(2)(b), 17(3)(b), 22, 26
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 Delivery Clerk	67205	14, 15, 17(2)(b), 17(3)(b), 22, 26
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*

Statistical Report on the *Privacy Act*

Name of institution: Employment and Social Development Canada
Reporting period: 2014-04-01 to 2015-03-31

Part 1: Requests Under the Privacy Act

	Number of Requests
Received during reporting period	7998
Outstanding from previous reporting period	552
Total	8550
Closed during reporting period	7781
Carried over to next reporting period	769

Part 2: Requests Closed During the Reporting Period

2.1 Disposition and completion time

Disposition of Requests	Completion Time							
	1 to 15 Days	16 to 30 Days	31 to 60 Days	61 to 120 Days	121 to 180 Days	181 to 365 Days	More Than 365 Days	Total
All disclosed	272	504	102	15	2	0	0	895
Disclosed in part	1221	4052	538	56	5	10	7	5889
All exempted	2	0	0	0	0	0	0	2
All excluded	1	2	0	0	0	0	0	3
No records exist	602	193	12	2	1	1	0	811
Request abandoned	92	42	11	6	8	14	8	181
Neither confirmed nor denied	0	0	0	0	0	0	0	0
Total	2190	4793	663	79	16	25	15	7781

2.2 Exemptions

Section	Number of Requests	Section	Number of Requests	Section	Number of Requests
18(2)	0	22(1)(a)(i)	0	23(a)	0
19(1)(a)	0	22(1)(a)(ii)	0	23(b)	0
19(1)(b)	0	22(1)(a)(iii)	0	24(a)	0
19(1)(c)	0	22(1)(b)	13	24(b)	0
19(1)(d)	0	22(1)(c)	0	25	0
19(1)(e)	3	22(2)	0	26	5437
19(1)(f)	3	22.1	23	27	33

20	0	22.2	0	28	0
21	0	22.3	0		

2.3 Exclusions

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

2.4 Format of information released

Disposition	Paper	Electronic	Other formats
All disclosed	867	0	0
Disclosed in part	5376	0	0
Total	6243	0	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	21905	18340	895
Disclosed in part	611877	581719	5889
All exempted	1	0	2
All excluded	4	0	3
Request abandoned	0	3031	181
Neither confirmed nor denied	0	0	0
Total	633787	603090	6970

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	852	12937	42	5365	0	0	1	38	0	0
Disclosed in part	4113	166775	1639	293882	98	59506	38	54931	1	6625

All exempted	2	0	0	0	0	0	0	0	0	0
All excluded	3	0	0	0	0	0	0	0	0	0
Request abandoned	174	423	5	978	1	519	1	1111	0	0
Neither confirmed nor denied	0	0	0	0	0	0	0	0	0	0
Total	5144	180135	1686	300225	99	60025	40	56080	1	6625

2.5.3 Other complexities

Disposition	Consultation Required	Legal Advice Sought	Interwoven Information	Other	Total
All disclosed	1	0	0	159	160
Disclosed in part	33	0	330	230	593
All exempted	0	0	0	0	0
All excluded	0	0	0	0	0
Request abandoned	0	0	0	0	0
Neither confirmed nor denied	0	0	0	0	0
Total	34	0	330	389	753

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
242	208	2	7	25

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	151	27	178
16 to 30 days	52	5	57
31 to 60 days	35	8	43
61 to 120 days	27	3	30

121 to 180 days	9	1	10
181 to 365 days	17	4	21
More than 365 days	5	9	14
Total	296	57	353

2.7 Requests for translation

Translation Requests	Accepted	Refused	Total
English to French	1	0	1
French to English	9	0	9
Total	10	0	10

Part 3: 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

Disposition for Correction Requests Received	Number
Notations attached	3
Requests for correction accepted	3
Total	6

Part 5: Extensions

5.1 Reasons for extensions and dispositions 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	24	0	0	0
Disclosed in part	179	0	7	11
All exempted	0	0	0	0
All excluded	0	0	0	0
No records exist	5	0	0	0
Request abandoned	9	0	0	0
Total	217	0	7	11

5.2 Length of extensions

Length of Extensions	15(a)(i) Interference with operations	15(a)(ii) Consultation		15(b) Translation purposes
		Section 70	Other	
1 to 15 days	0	0	0	1
16 to 30 days	217	0	7	10
Total	217	0	7	11

Part 6: Consultations Received From Other Institutions and Organizations

6.1 Consultations received from other Government of Canada institutions and other organizations

Consultations	Other Government of Canada Institutions	Number of Pages to Review	Other Organizations	Number of Pages to Review
Received during the reporting period	11	682	0	0
Outstanding from the previous reporting period	0	0	0	0
Total	11	682	0	0
Closed during the reporting period	10	199	0	0
Pending at the end of the reporting period	1	483	0	0

6.2 Recommendations and completion time for consultations received from other Government of Canada institutions

Recommendation	Number of Days Required to Complete Consultation Requests							
	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	8	0	0	0	0	0	0	8
Disclosed in part	0	2	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	8	2	0	0	0	0	0	10

6.3 Recommendations and completion time for consultations received from other organizations

Recommendation	Number of days required to complete consultation requests							
	1 to 15 Days	16 to 30 Days	31 to 60 Days	61 to 120 Days	121 to 180 Days	181 to 365 Ddays	More Than 365 Days	Total
All disclosed	0	0	0	0	0	0	0	0
Disclosed in part	0	0	0	0	0	0	0	0
All exempted	0	0	0	0	0	0	0	0
All excluded	0	0	0	0	0	0	0	0
Consult other institution	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0

Part 7: Completion Time 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
18	3	8	0	29

Part 9: Privacy Impact Assessments (PIAs)

Number of PIA(s) completed	7

Part 10: Resources Related to the *Privacy Act*

10.1 Costs

Expenditures		Amount
Salaries		$3,400,814
Overtime		$65,631
Goods and Services		$340,597
• Professional services contracts	$184,300	
• Other	$156,297	
Total		**$3,807,042**

10.2 Human Resources

Resources	Person Years Dedicated to Privacy Activities
Full-time employees	26.36
Part-time and casual employees	3.34
Regional staff	34.65
Consultants and agency personnel	2.00
Students	0.76
Total	**67.11**