Office of the
Privacy Commissioner
of Canada

AUDIT REPORT OF THE PRIVACY COMMISSIONER OF CANADA

Privacy Management Frameworks of Selected Federal Institutions

Section 37 of the *Privacy Act*

2009

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP54-20/2009
ISBN 978-0-662-06496-1

This publication is also available on our Web site at **www.privcom.gc.ca**.

Table of Contents

Foreword

Canadians and residents of Canada come in contact with the federal government in several ways. They receive services and benefits such as income security and Canada Pension Plan payments; they exercise their rights—the right to vote, for example, and to move freely in and out of the country; and they fulfill obligations such as the requirement to pay taxes. The various federal organizations that deliver these services, benefits and rights have to confirm that their clients are the people they claim to be.

Confirming a person's identity every time they deal with government is a complex business challenge. Many people use slight variations of their names or record their dates of birth in different ways. Each year, enormous numbers of Canadians move to new addresses. And people forget or misplace the identifying numbers assigned to them and the passwords that they have created.

To meet this challenge, federal organizations collect information from the same people for different purposes—information that is similar, though not always exactly the same from one organization to another.

Several recent audits by the Office of the Auditor General found that organizations managing this similar information faced similar challenges. In the spring of 2007, the Office decided to look more closely at how federal organizations manage the information that they use to identify their clients—their 'identity' information. The Office was particularly interested in how they ensure the quality of the information and to what extent they collaborate to ensure the efficient use of the government's information holdings.

The Office of the Privacy Commissioner has also conducted several audits of how federal institutions are managing the personal information they hold, which includes identity information. It found that institutions need a robust privacy management framework if they are to achieve their program objectives and observe best privacy practices. The Commissioner's Office decided to look more closely at the privacy management frameworks of certain federal institutions: how they organize themselves through structures, policies, systems and procedures to distribute privacy

responsibilities, coordinate privacy work, manage privacy risks, and ensure compliance with the *Privacy Act*.

Our two offices therefore agreed to work collaboratively on concurrent audits, consistent with our respective mandates. This collaboration represents a historic first: audits of selected federal institutions, conducted and reported on concurrently by two Officers of Parliament.

The two audit teams participated jointly in audit-related processes and shared information on a regular basis.

Both offices report on the systems and practices of four federal institutions, each of which manages at least one large database of personal information that includes identity information. Elections Canada, for example, manages the National Register of Electors, which contains the personal information of about 23 million eligible Canadian voters. Service Canada manages the Social Insurance Register, with the personal information of everyone who has applied for a Social Insurance Number; the Register held nearly 31 million active records in 2007. The Canada Revenue Agency manages the IDENT database containing the personal information of about 33 million individual taxpayers, and Passport Canada's Central Index contains records of more than 17 million active passports.

The Office of the Auditor General found that, with one exception, the organizations collected only the identity information they are authorized to collect. The quality of the collected information is managed well in two of the federal institutions, while there are opportunities to improve in the two others. However, federal institutions have not integrated their approaches to managing identity information. Many similar frameworks, strategies, and initiatives have been pursued over the past 10 years, but the result has been some duplication of process, frequent reconsideration of the same problems, and incomplete solutions to the underlying needs.

The Office of the Privacy Commissioner found that the privacy management frameworks of two of the four federal institutions are reasonably robust, but require improvement, while there are significant gaps with respect to the way personal information is managed by two other institutions. It found instances where personal information is being collected and used without legislative authority, where personal information is at risk of unauthorized disclosure or loss, or where privacy risks were not appropriately assessed. Weaknesses in an institution's privacy management framework can have a variety of real consequences for Canadians, including the risk that personal information will be used for illegal activities such as identity theft.

Both Officers of Parliament call for stronger leadership from the centre of government—specifically, the Treasury Board Secretariat. The Secretariat has a critical role to play in setting standards and issuing policy, directives, and guidance on managing identity information and developing model frameworks for privacy management.

Without stronger leadership, federal institutions will likely continue independently to develop incomplete solutions to their common challenges: how to authenticate the identity of the Canadian citizens and residents they serve; and how to ensure the privacy of the personal information they collect and use, including its integrity, security, and confidentiality. The full picture of the opportunities—and the risks of inaction—emerges in reading the two reports as a whole.

Federal institutions can do a better job of managing the personal information assets of government. Failure to do so will be costly and inefficient and could erode the privacy of Canadians.

Original signed by

Sheila Fraser
Auditor General of Canada

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Executive Summary

1.1 The Office of the Privacy Commissioner (OPC) examined key elements of the privacy management frameworks of Elections Canada, Human Resources and Social Development Canada (HRSDC)/ Service Canada, and the Canada Revenue Agency (CRA). Collectively, these institutions manage extensive personal information on just about everybody in Canada.

1.2 In a separate audit, we also examined elements of the privacy management framework of Passport Canada. We have already issued our audit report of Canadian Passport operations. As the observations with respect to the privacy management framework of Passport Canada are germane to the current audit, they have been included as an appendix to this report (See Appendix B). The conclusions of this audit also draw on the observations that were made about Passport Canada.

1.3 By a privacy management framework, we mean the way in which institutions organize themselves through structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and ensure compliance with the *Privacy Act*. Federal institutions with weak privacy management frameworks may risk losing the confidence of Canadians.

1.4 Each of the institutions we examined is at a very different stage of maturity with respect to its privacy management framework. We noted examples of positive privacy practices. We also identified examples of poor practice. We believe poor practices could have been avoided, had stronger privacy management frameworks been in place. We found instances where:

- personal information is being collected and used without legislative authority,
- personal information is being collected, where the institution had not formally considered whether it was needed,
- personal information is at risk of unauthorized disclosure or loss,

- privacy risks were not assessed when significant changes to business practices were introduced.

1.5 All the institutions we examined use formal agreements to manage their information collection and sharing arrangements with other federal institutions. This is a positive practice that exceeds the requirements of the *Privacy Act* and the current policy guidance of the Treasury Board of Canada Secretariat (TBS). However, we identified some shortcomings in the management of the agreements. We recommend that the institutions:

- continue to use formal mechanisms, such as information sharing agreements, in all instances where they collect and/or disclose personal information,
- ensure their information sharing agreements are reasonably current,
- ensure that they are developed within a framework of modern guiding privacy principles, and
- ensure that they are reviewed and subject to independent measures of assurance.

1.6 We identified pressures and gaps with respect to privacy training. This is consistent with the results of a recent government wide survey conducted by the Treasury Board Secretariat (TBS) which indicated that Access to Information and Privacy (ATIP) offices are reporting a need for more privacy training for their professional staff. They also reported that they face challenges in delivering privacy training to their employees.

1.7 We recommend that the institutions strengthen their privacy training programs. We also suggest that in addition to its ongoing privacy training for members of the Access to Information and Privacy community, TBS lead the development and promotion of a core privacy training curriculum for all public service employees.

1.8 We found that the institutions have ATIP Offices that are to varying degrees focused on meeting the legislated timeframes for access requests, and on responding to and dealing with individual inquiries and complaints. The pressures of these transactional demands make it difficult for ATIP Coordinators to assume a strategic privacy leadership role.

1.9 In three institutions, we recommend the appointment of a Chief Privacy Officer. One institution already has a Chief Privacy Officer.

1.10 We would have liked to have independently assessed and reported on how TBS discharges its obligations under the *Privacy Act (*the *Act),* and monitors compliance. However, under a strict interpretation of the *Act*, the Privacy Commissioner does not have the authority to do so.

1.11 We were advised by TBS that it monitors all institutions subject to the *Privacy Act* through public accountability instruments: Annual Reports to Parliament, *Info Source* publications, personal information banks and statistical reports. It also subjects approximately twenty percent of the institutions to more intensive scrutiny. This is still essentially limited to a review of public reporting obligations, and may not reflect actual privacy performance. In this limited regard, TBS did not rate accountability for privacy as strong for any of the 46 institutions that it recently reviewed. This is a disappointing result.

1.12 Several important opportunities exist where TBS could strengthen privacy management across the federal government. These include:

- issuing directives to implement recently revised privacy policies,
- implementing a new policy on privacy impact assessments,
- developing policy and guidance on identification and authentication,
- leading the development and promotion of a core privacy training curriculum for government employees,
- establishing effective guidance on the sharing of personal information between federal institutions and agencies, and between levels of government, and
- creating a model privacy management framework for institutions.

1.13 We were advised by TBS that in the context of its review and renewal of privacy policies, it intends to address issues of governance, risk management, training and awareness, program monitoring and reporting, and administration of the *Privacy Act*. Such an initiative is welcome and needed.

1.14 In conclusion, there are significant opportunities to strengthen the privacy management frameworks of federal institutions in order to assure Canadians that their privacy rights are fully served.

Introduction

1.15 As many as two hundred and fifty (250) federal government institutions are subject to the *Privacy Act (*the *Act)* with regard to the management of the personal information that they collect and use in providing services to Canadians.

1.16 The designated head of the institution, often a Minister or Chief Executive Officer, is responsible for compliance. He or she must report annually on the administration of the *Act*, and ensure, for example, that the institution discharges the various obligations set out in sections 4 to 8 of the *Act*.

1.17 Although the *Act* does not require the head of an institution to establish a framework of management controls, systems or procedures, a privacy management framework is clearly needed if the institution is to ensure compliance with statutory privacy obligations and observe good privacy practices.

1.18 In this audit, the OPC used modern privacy principles to develop audit criteria. We examined key elements of the privacy management frameworks of institutions that the Office of the Auditor General (OAG) had chosen for examination: Elections Canada, HRSDC/ Service Canada, and the Canada Revenue Agency. The OAG also chose Passport Canada for examination. We had already begun a comprehensive audit of Passport Canada, one which included an examination of elements of its privacy management framework. As the observations with respect to its privacy management framework are relevant to this audit, we have included them, for ease of reference, in Appendix B. Collectively, the four institutions manage extensive personal information on just about everybody in Canada.

1.19 There are important differences between these institutions. Each delivers a very different service or services to Canadian residents, operating under specific and unique legislative authorities. They are dramatically different in size and complexity.

1.20 All of these institutions face common challenges in fulfilling their privacy and security obligations and their business objectives. They need to collect the personal information of Canadian residents to

determine their eligibility for specific services and programs, and, in the case of the CRA, to assess their tax liability. All of these institutions must ensure the integrity and security of the information that they exchange, as well as the information that they hold. All of them recognize the importance of the confidentiality of personal information.

1.21 But security and client confidentiality are not, in and of themselves, synonymous with privacy. Privacy means, among other things, limiting the collection of personal information to that which is necessary for the purposes of a specific program or service. It means using information in a manner which is consistent with the purpose for which it was originally collected. It means being open and transparent about privacy practices. It means providing the individual with a right of access to his or her personal information, and the right to ensure that the information that will be used to make an administrative decision about that individual is accurate. It also means finding the appropriate balance between the individuals' right to anonymity, and the program's need to identify an individual and authenticate his or her right to services. A strong privacy management framework would help to achieve these expectations.

1.22 As part of a privacy management framework, all of these institutions also need to provide their employees with privacy training, both those employees who provide face-to-face, over the counter or telephone service, and the managers who are ultimately held to account for the institution's privacy practices. They all need to deal with the challenge of aging technological platforms which may not meet emerging business needs, such as e-government, and with new threats to security posed, for example, by increasingly sophisticated internet hackers.

1.23 The Executive Summary of this report provides a synopsis of the key findings and conclusion of this audit. The remainder of this report details our observations and recommendations specific to each entity scoped for examination. It also provides information regarding the role and work of the Treasury Board Secretariat (TBS).

1.24 The effective date of these observations and recommendations is June 30, 2008. This marked the end of our examination work, and the date when this report was first drafted. We wish to thank management and staff of all the institutions for their cooperation and responsiveness.

Audit Scope and Criteria

1.25 We used a number of sources to develop the evaluation criteria used in this audit[1]. As noted earlier, they reflect modern privacy principles and best practices that are not enshrined in the *Privacy Act*. For example, we developed criteria based on the Canadian Standard Association's *Model Code for the Protection of Personal Information*[2]. We also adapted the Canadian Institute of Chartered Accountants guidance document, entitled *Generally Accepted Privacy Principles*. It was developed "to help management create an effective privacy program that addresses privacy risks and obligations and business opportunities".

1.26 We expected federal institutions subject to the *Act*:

- to have a governance and accountability structure that ensures the effective coordination of the privacy related responsibilities of front-line staff, managers, and security, information technology, and privacy specialists,
- to ensure that all employees with privacy responsibilities have privacy and security training,
- to have systems and procedures in place to identify, monitor and mitigate privacy risks related to new or proposed programs and services, and to ongoing operations,
- to adopt an integrated set of privacy policies, based on existing models and best practices, to guide their business practices,
- to set privacy standards, targets and measures, and
- to regularly monitor and report on their achievement.

1 The OPC developed audit objectives and criteria specific to its separate, comprehensive review of Passport Canada's operations. These included an examination of elements of its privacy management framework, as set out in this report. Please refer to the audit of Passport Canada, available at: www.privcom.gc.ca, for more detailed information on the approach taken in auditing Passport Canada operations.

2 TBS also adapted the *Model Code* to develop its Privacy Impact Assessment policy.

1.27 We did not attempt to prescribe every element of a privacy management framework, nor did we examine privacy practices in detail within each of the institutions scoped for examination. Treasury Board Secretariat is, in our view, responsible for providing guidance to federal institutions subject to the *Act*, including the development of model privacy management frameworks. For more information about the audit, see **Appendix A** at the end of this report.

Observations and Recommendations

Elections Canada

Introduction

2.1 Elections Canada is an independent, non-partisan agency that reports directly to Parliament. It has approximately 400 full time, permanent employees in the National Capital Region.

2.2 Prior to 1997, when an election was called, Elections Canada conducted a door to door enumeration to create a list of eligible voters. The voters' lists consisted of the names and addresses of eligible voters, information that most Canadians would likely not consider particularly sensitive. The lists were and still are used to control access to the voting process, ensuring that a person entitled to vote casts his or her ballot in the right polling division within the right electoral district.

2.3 The *Canada Elections Act* was amended in 1997 to allow for the creation of a permanent voters' list, the National Register of Electors (NRE). The NRE contains the personal information of approximately 23 million eligible Canadian voters. Under section 44(3) of the *Canada Elections Act*, inclusion in the NRE is at the option of the elector, and Elections Canada advises on its website that it embraces the principle of "active, informed consent" with respect to the NRE.

2.4 Elections Canada conducted a final enumeration of electors to populate the NRE in 1997. To remain current, the NRE must be updated on an ongoing basis: as young Canadians turn eighteen and become entitled to have their names included on the Register, as a significant number of Canadians move each year within their electoral district or from one electoral district to another, to include the personal information of new Canadians, and to remove the names of voters who have died.

2.5 Elections Canada updates the NRE using personal information it obtains from various provincial, territorial and federal partners. It collects information from more than forty provincial and territorial sources, named in a Schedule to the *Canada Elections Act*. It collects vital statistics (information about deaths only) and driver's licence information, information from the Canada Revenue Agency (from consenting tax filers), from Citizenship and Immigration Canada (to capture information about new Canadians), and address changes from Canada Post (the National Change of Address Database). It also has agreements to exchange information with provincial electoral bodies and municipal partners, for the purpose of updating the NRE.

2.6 Canadians will be most familiar with the key mechanism used to update the NRE, the tick-off boxes on their income tax return form that ask them to consent to the sharing of their name, citizenship, address and date of birth with Elections Canada.

2.7 In addition to the names, and current and previous addresses of voters, the NRE holds information about a voter's date of birth, gender, driver's licence number, and any unique identifying numbers assigned by the institutions that provide personal information to Elections Canada.

2.8 As permitted by the provisions of section 73 of the *Privacy Act*, the Chief Electoral Officer has delegated his privacy responsibilities to an Access to Information and Privacy (ATIP) Coordinator.

Why the audit is important

2.9 There have been a number of important changes to the electoral process, as a result of recent amendments to the *Canada Elections Act*. Most of these changes came into force on March 1, 2008, for elections called subsequent to that date.

2.10 First, when voters go to a polling station, they will be required to present documents to prove that they are who they say they are, and to prove that they live within the boundaries of the polling division where they want to vote.

2.11 Secondly, the Chief Electoral Officer is now required to assign a unique, randomly generated personal identifier to each person registered in the NRE, and to disclose that identifying number to candidates during an election, and to political parties and members of Parliament on a yearly basis.

2.12 According to a report of the Chief Electoral Officer, the unique identifier will make it easier for political parties to integrate the

lists of electors into their own internal party lists[3]. About 23 million Canadians (about 76% of the total population of Canada) will have a unique number assigned to them, a permanent identifier which will be disclosed, along with their names and current address, to political parties and federal candidates.

2.13 While registered political parties receive a complete list for those ridings in which they ran a candidate in the previous election, individual candidates and MPs only receive a list of the constituents who live within their riding. The lists are distributed both in a paper format (up to five paper copies per electoral candidate) and on CD-ROMs that are password protected and encrypted. The voters' lists were distributed to 1,634 candidates during the 39th General Election of January, 2006.

2.14 As well, the *Canada Elections Act* has been amended to require the disclosure of an eligible voter's full date of birth on the lists of electors that are distributed to deputy returning officers and poll clerks. The elector's date of birth is to be used as a control mechanism to ensure that only eligible persons are allowed to vote at a particular polling station.

2.15 Election activities within the electoral districts and at polling stations are directed and managed by Returning Officers. Up until 2007, Returning Officers were appointed by the government in power, through an order of the Governor in Council. The 308 electoral districts were, according to the Report of the Chief Electoral Officer[4], independent and separate entities, not subject to the basic machinery of government statutes, such as the *Privacy Act.* As a result of the recent amendments to the *Canada Elections Act*, passed in June, 2007, Returning Officers are now under the authority of the Chief Electoral Officer, and the temporary workers that they hire during an electoral event are, apparently for the first time, subject to the *Privacy Act*[5].

2.16 During an election event, the Returning Officers hire approximately 190,000 temporary election workers to staff approximately 65,000 polling stations in 308 electoral districts. For each polling station, a deputy returning officer and poll clerk are required to verify the identity and address of electors and administer the vote. The list of electors provided to them would contain the first and last names, civic and mailing addresses, gender, date of birth, and unique personal identifier of eligible voters who live in their polling division. The lists contain, on average, 350 names.

---

3 *Completing the Cycle of Electoral Reforms – Recommendations from the Chief Electoral Officer*, CEO of Canada, 2005, p. 62.

4 Ibid, pp. 14-15.

5 However, political parties and their candidates are not subject to the *Privacy Act*.

2.17 The increased risk associated with the inclusion of the date of birth and a unique identifier on voters' lists used by election workers on polling days underline the importance of building an effective privacy management framework, to reduce to a minimum the risk that the personal information of Canadians will be used for purposes other than those permitted by law. The Privacy Commissioner of Canada expressed concern about this risk when she was asked in May, 2007 for her views about the proposed changes to the *Canada Elections Act*.

What we found

2.18 We found that Elections Canada is aware of privacy as an important consideration in the programs they deliver and in their business activities. The written materials that are distributed to stakeholders during an election event and posted on the Elections Canada website reference the importance of privacy.

2.19 Elections Canada has undertaken some positive measures to mitigate privacy and security risks; for example, the introduction of a privacy awareness training program for election event workers, and the encryption and password protection of the electoral lists that are distributed on CD-ROMs to the candidates during an electoral event.

2.20 The design of Elections Canada's security measures with respect to the internal management of the NRE is adequate. Elections Canada has implemented a set of safeguards and control procedures to ensure the secure collection and/or exchange of personal information with its federal, provincial, and territorial partners, and to safeguard the information holdings in the NRE.

2.21 As permitted by section 73 of the *Privacy Act*, the Chief Electoral Officer has delegated the privacy responsibilities of the head of the institution to the Access to Information and Privacy (ATIP) Coordinator of Elections Canada.

Governance structure and accountability measures need to be strengthened

2.22 As a result of amendments to the *Federal Accountability Act*, Elections Canada first became subject to the *Access to Information Act* in 2007. The structure of the ATIP office has been determined, and TBS recently approved funding for 4 positions.

2.23 According to Elections Canada, the ATIP Office will be able to manage the anticipated volume of access to information and privacy requests. It is not clear that the ATIP Office will have the capacity to manage critical privacy practices, such as privacy impact assessments, policy development, training, or privacy breach reporting.

2.24 The ATIP Coordinator is the only position at Elections Canada with defined privacy responsibilities, and the ATIP Office has developed a high level work plan. The ATIP Office does not currently have a formal process, procedures, or timelines for dealing with privacy issues or concerns.

2.25 There are other management positions within Elections Canada that have significant privacy responsibilities. The Returning Officers in each of the 308 Electoral districts have overall responsibility for the privacy and security of the electoral documentation and lists entrusted to them. The Senior Director, Field Readiness and Event Management, oversees the conduct of an election by local offices and as such makes sure that elector data products reach their destinations. The Senior Director, Electoral Data Management Readiness is responsible for the safe transmission of data products to parties and MPs, and for relationships with federal, provincial and municipal data suppliers and electoral partnerships. This position is, per TBS policy, responsible for ensuring that there are appropriate privacy protection clauses in intergovernmental agreements.

2.26 It appears that the ATIP Coordinator is currently working with other senior managers in an ad hoc way, without clearly defined performance targets or protocols to determine how and by whom privacy responsibilities will be discharged.

2.27 Elections Canada advised us that it is preparing a more detailed privacy work plan. We agree that one is required. Elections Canada should consider including in its privacy work plan specific deliverables and timeframes, such as a process, procedures, and timelines for dealing with privacy issues or concerns.

Recommendation

2.28 It is recommended that Elections Canada strengthen its privacy governance structure and accountability for privacy. Elections Canada should consider:

- setting out the privacy related performance expectations of the ATIP Coordinator and other senior managers within Elections Canada in the performance agreements of each manager,
- establishing formal protocols to determine how, when, and under what circumstances the ATIP Coordinator will provide privacy advice regarding the business activities of the operations managers, and
- appointing a Chief Privacy Officer to provide strategic privacy leadership, and to oversee and coordinate the privacy work of the ATIP Coordinator and the managers who have privacy responsibilities.

Management Response

Elections Canada recognizes the importance of the elector information entrusted to it as this information is central to the administration of the electoral process. Security of personal information has always been a priority because it is essential to preserving elector confidence in that process. We welcome the observations of the Office of the Privacy Commissioner of Canada in relation to strengthening the governance and accountability for privacy.

Consequently, we will review our internal governance structure and determine how best to design a privacy management framework that will assure continued compliance with the ***Privacy Act*** *and with TBS guidelines and policies.*

Privacy training

2.29 As noted, during the past year, the ATIP Coordinator has begun to provide privacy training to the Returning Officers, who are responsible for managing elections at the local level. This initiative is important, and commendable. In June, 2008, two of the senior managers of Elections Canada received a presentation on the basics of privacy.

Recommendation

2.30 It is recommended that Elections Canada's continue a program of mandatory privacy training for managers and all employees who handle personal information or have privacy responsibilities.

Management Response

Elections Canada will continue to deliver and expand its privacy training.

Enterprise-wide program delivery coordination and risk management mechanisms need to be formalized, and incorporated into the governance framework

2.31 According to the TBS Policy on Privacy Impact Assessments, departments are required to institute a formal process to identify and mitigate privacy risks when introducing new programs or services. Under the provisions of the policy as it is currently written, the recent amendments to the *Canada Elections Act*, allowing for the distribution of a unique identifier and an elector's date of birth, triggered a requirement that a PIA be considered. Elections Canada concluded that a PIA was not required as the changes flowed from legislative amendments. In our view, a PIA should have been done.

2.32 During our examination, we also determined that Elections Canada has initiated a substantial revision of its business practices regarding the special voting rules (and lists). A Threat and Risk Assessment of the new business practices was conducted. According to the PIA

policy, Elections Canada was also required to consider the need for a privacy impact assessment in the early stages of this initiative. Elections Canada did consider the need, and determined that one was not necessary[6]. In our view, a PIA should have been done.

2.33 The ATIP Coordinator has proposed that the terms of reference of the Information Management/Information Technology Committee be amended to include a responsibility to coordinate and manage privacy and security risks related to the introduction of new programs or services (through the Privacy Impact Assessment process). At the time of our audit, no final decision had been taken in this regard.

Recommendation

2.34 It is recommended that Elections Canada implement measures to ensure that privacy impact assessments are considered for all new program initiatives.

Management Response

Elections Canada agrees that privacy impact assessments (PIAs) must be considered for all new program initiatives and will establish procedures to ensure that PIAs are part of the normal project life cycle. We anticipate that procedures for ensuring that PIAs are considered as part of each new initiative will be in place by March 31, 2009.

Privacy risks in ongoing operations need to be addressed

2.35 Privacy risks also arise from ongoing operations. We reviewed the guidance that Elections Canada provides to the electoral workers, election candidates, and political parties that receive voters' lists. The *Guidelines on Disclosure and Use of the Lists of Electors* stress the importance of protecting the privacy of the personal information on the lists. They recommend that the recipients of the list appoint a person to be responsible for communicating the guidelines to others, such as political party workers or the staff of MPs, who will have access to the lists. They also point out that it is an offence under the *Canada Elections Act* to knowingly use the list of electors for other than electoral purposes.

2.36 Political parties, MPs, and candidates are not required by either the *Canada Elections Act* or the *Privacy Act*, or requested by the Guidelines, to report any loss or inappropriate use of the electoral lists. In our view, it would be good practice if they were to report to Elections Canada

6 The Chief Electoral Officer is responsible for deciding whether or not a PIA is required. It appears that he was not consulted in this instance.

any loss of the electoral lists that are distributed to them by Elections Canada.

2.37 Elections Canada indicated that there have only been four known privacy breach incidents in the past several years. We reviewed the management of three of the privacy breaches at Elections Canada. It was clear from a review of the files that Elections Canada treats privacy breaches seriously, and in one instance in particular, it made sustained efforts to prevent further breaches.

2.38 However, Elections Canada does not have an internal policy on breach reporting, it does not set reporting obligations for its managers and staff, and it does not have any systematic means of identifying privacy breaches.

2.39 A comprehensive approach to privacy breach reporting can help departments to better manage privacy risks, allowing them to adjust their business operations based on lessons learned.

2.40 In 2003, TBS issued *Guidelines for Privacy Breaches*, to help departments avoid instances of improper or unauthorized access to or disclosure of personal information, and to mitigate the consequences of a breach, should one occur.

2.41 One of the breach files that we reviewed involved the personal information of an employee of Elections Canada. Two others involved electoral lists. One of the two has attracted media attention: the RCMP's discovery in 2006 that lists containing the names and addresses of voters were found in the offices of a Tamil Tiger cell, a listed terrorist entity. The RCMP is alleging that the lists were being used to identify potential financial contributors to the Tamil cause. According to media reports, the lists in question were candidate's lists.

2.42 The third privacy breach file that we reviewed involved the personal information of electors under the control of Elections Canada. As a result of concerns expressed by some parliamentarians regarding the extent of polling day registration in the electoral district of Trinity Spadina during the 39th general election, the Office of the Chief Electoral Officer commissioned a special study. The consultants who undertook the study determined that election documents, such as Official Lists of Electors, poll books, electronic data storage tapes, and registration certificates could not be located. While the Official Lists of Electors contained only the names and addresses of electors, the registration certificates included former addresses and dates of birth. Elections Canada subsequently redesigned training programs, enhanced procedural documentation, and introduced additional control measures which it tested in subsequent by-elections.

2.43 According to Elections Canada, between four and twelve percent of the poll books and electoral lists (depending on the electoral district)

used at polling stations in by-elections held in September, 2007, could not be accounted for. Elections Canada advised us that in by-elections held in March, 2008, the overall percentage of electoral documentation that could not be found improved. Elections Canada concluded, based on a limited sampling of only three electoral districts, that slightly more than 1 per cent of electoral documentation could not be accounted for. However, the actual number of known official lists that could not be located was the same in March of 2008, as it was in the Trinity-Spadina riding during the 39th general election of January, 2006: on both occasions, ten official lists of electors could not be located.

2.44 It appears to be very difficult to control and fully account for electoral documentation. A solution to this problem may well require a reconsideration of governing legislation.

2.45 There was a delay in reporting the privacy breach to the OPC. This issue first arose in the spring of 2007. In June, 2007, Elections Canada determined that in order to comply with the TBS *Guidelines for Privacy Breaches*, its ATIP Coordinator should notify the OPC. The Chief Electoral Officer verbally advised the Privacy Commissioner of the incident in March, 2008. At the time of completing our audit examination in June 2008, more than one year later, the OPC had yet to be formally advised. This is not consistent with TBS guidelines.

2.46 Subsequent to completing our audit examination, a notification letter dated July 2, 2008 was received in the Office of the Privacy Commissioner on July 8, 2008. The Chief Electoral Officer indicated that his office would pursue solutions to the problem.

Recommendations

2.47 It is recommended that Elections Canada:

- develop an internal privacy breach reporting policy, and train its employees on the policy's obligations,
- include, in its *Guidelines on Disclosure and Use of the Lists of Electors*, a mechanism whereby election workers, political parties, MPs, and electoral candidates can report and receive advice regarding the loss of an electoral list, and,
- develop a mechanism whereby senior management can regularly review privacy breach incidents and determine if corrective measures are needed to prevent future incidents.

2.48 It is recommended that Elections Canada ensure that it complies with the breach reporting expectations set out by the Treasury Board Secretariat.

2.49 It is also recommended that Elections Canada continue to pursue ways to mitigate risks associated with the distribution of electoral information.

Management Response

Elections Canada will continue to pursue a range of risk-mitigating measures for the protection of elector information.

We are currently considering revisions to the Guidelines on Disclosure and Use of the Lists of Electors, which we distribute with the annual release of the lists to parties and members of Parliament, as well as with the lists of electors that we provide to political parties and candidates during an election. Any changes to these guidelines will be implemented prior to the distribution scheduled for November 2009.

With respect to reporting, we note that the study on polling day registration in Trinity-Spadina was published on May 1, 2007, posted on Elections Canada's Web site and filed with the Standing Committee on Procedure and House Affairs. Elections Canada acted transparently and took corrective action to protect the privacy of electors. Elections Canada will continue to follow the breach-reporting expectations set out in the Treasury Board Secretariat's guidelines and will ensure that improved mechanisms for employee awareness and compliance as well as management oversight are implemented by December 31, 2009.

Meaningful consent

2.50 While the *Privacy Act* only requires that the individual be notified of the purposes for which personal information is being collected, the *Canada Elections Act* has a higher standard. It specifically provides that inclusion in the Register of Electors is "at the option of the elector". Voters consent to having their name and personal information held in the NRE, and they explicitly consent to the sharing of their personal information between federal departments (such as the Canada Revenue Agency) and Elections Canada. Elections Canada is committed to applying the principle of "active, informed" consent.

2.51 Consent is a key principle in the *Model Code for the Protection of Personal Information*, referenced earlier. The principle requires that organizations obtain the meaningful consent of the individual by bringing to the attention of the individual its proposed collection, use and disclosure practices, at the time of collecting personal information. According to the principle, an organization needs to describe its proposed practices in language that a reasonable person can understand, advise the individual of the consequences of not providing consent, and of how the individual can withdraw consent.

2.52 Elections Canada does provide information on its website about the permitted uses of personal information (per the provisions of the *Canada Elections Act*), and about how voters can have their personal information removed from the NRE.

2.53 Electors who have had their personal information removed from the NRE can still choose to vote during an election. If they do, in spite of the fact that they have requested that they be removed from the NRE, the *Canada Elections Act* requires that their personal information be included on the final list of electors that is distributed to the political parties.

2.54 Tax filers who are completing their income tax return form have the option of explicitly authorizing the sharing of their name, address, date of birth and citizenship with Elections Canada. The tax form advises the taxpayer that the information will be used for purposes permitted under the *Canada Elections Act*. However, the current version of the consent document does not tell the consenting taxpayer what personal information will be disclosed and to whom, and it does not alert the taxpayer to the precise nature of the purposes permitted under the *Canada Elections Act*. It also does not refer the tax filer to a source where he or she can obtain further information, specifically with respect to the consequences of not providing consent, and on how to opt-out of the NRE. As a result, meaningful consent is not achieved.

Recommendation

2.55 It is recommended that Elections Canada strengthen its practices to ensure that it obtains the meaningful consent of electors.

Management Response

Elections Canada is reviewing its Web site and public information, including consent documentation relating to the Register of Electors. Where appropriate, changes will be made to ensure that electors are adequately informed regarding how their personal information is collected, use and disclosed and that they understand that they may opt out of the Register without jeopardizing their right to vote. The review of the Web site and other public information related to the Register of Electors will be completed by December 31, 2009.

Information collection and sharing agreements

2.56 Elections Canada collects (but does not share) information from provincial vital statistics and driver's licence agencies, from the Canada Revenue Agency, from Citizenship and Immigration Canada, and from Canada Post, for the purposes of updating the NRE. It is permitted to do so by the provisions of section 46 of the *Canada Elections Act*. Subsection 46(1)(a) permits the Chief Electoral Officer, with the express authority of an elector, to update the NRE based on information held by a federal department[7]. Elections Canada has formal agreements governing these collection practices, with both provincial and federal organizations. The provisions of the agreements vary. Some have been relatively static, while others have been regularly reviewed. All of the agreements contain very detailed provisions regarding the security and protection of the information. The security provisions were introduced into the agreements approximately eight years ago.

2.57 The Treasury Board Policy on the Collection of Personal Information states:

> The policy requires that institutions have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. This means that institutions must have parliamentary authority for the relevant program or activity, and a *demonstrable need* (emphasis added) for each piece of personal information collected in order to carry out the program or activity.
>
> As well, Section 4 of the *Privacy Act* indicates that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

2.58 We found that Elections Canada has been receiving the personal information of 16 and 17 year old drivers from some provincial motor vehicle registrars, although it was not seeking this information. It has been contacting these drivers once they turn 18 to determine their interest in being added to the NRE. In our view, Elections Canada does not have the legislative authority to collect information about 16 and 17 year old drivers.

7 The *Canada Elections Act* does not require electors to consent to Elections Canada's collection of information from provincial government agencies.

2.59 Elections Canada has also been automatically receiving other information that it was not seeking, such as the status of a person's driver's licence (i.e., valid or not). It does not need or use this information to update the NRE.

2.60 Elections Canada also exchanges the personal information of electors with provincial, territorial and municipal electoral bodies. Section 55 of the *Canada Elections Act* authorizes these exchanges, and requires the Chief Electoral Officer to enter into formal agreements with the provinces that contain conditions regarding the use and protection of personal information.

2.61 Elections Canada uses a standard template for its information sharing agreements, a Memoranda of Understanding (MOU) which was last revised approximately 8 years ago. Elections Canada has not subsequently reviewed the privacy and security provisions of its information collection and sharing agreements.

2.62 The Privacy Subcommittee of the Institute of Citizen-Centred Services has issued a document entitled *Government- to-Government Information Sharing Agreements – Guidelines for Best Practice*, on behalf of the Public Sector CIO (Chief Information Officer) Council. The Council is comprised of CIOs from federal, provincial, territorial and municipal jurisdictions. TBS assisted in the development of the Guidelines. The *Guidelines* were issued "as a means of providing effective strategies to minimize or eliminate privacy risks within personal information sharing agreements". In our view, the *Guidelines* are valuable and applicable with respect to all information collection and sharing practices.

2.63 While Elections Canada's MOUs contain a provision allowing it to audit the data handling practices of other electoral bodies, Elections Canada has never used this provision.

Recommendation

2.64 It is recommended that Elections Canada cease collecting personal information (1) which the agency has no legislative authority to collect and (2) that it does not need or use. Elections Canada should implement measures to ensure that it is only collecting information that it is authorized to collect, consistent with the provisions of the *Canada Elections Act* and section 4 of the *Privacy Act*.

Management Response

Elections Canada has legislative authority to maintain and update personal information on qualified electors for electoral purposes. A qualified elector is a Canadian citizen who is 18 years of age or older on election day. Elections Canada has received the personal information on some individuals who are not yet 18 years of age and are therefore not qualified electors. We note, however, that information on these individuals has not been included in the National Register of Electors or on lists of electors. Elections Canada agrees with the recommendation and will take the following steps to comply by March 31, 2009:

- *Elections Canada will purge from its database all information on individuals under 18 years of age.*
- *Elections Canada will contact its suppliers to request that they provide information only for individuals 18 years of age or older. Until they have implemented this change, Elections Canada will filter the files received from its suppliers and will remove the records of individuals under 18 years of age before processing the files.*

However, pursuant to subsection 540(2) of the Canada Elections Act, Elections Canada is required to keep for at least two years documents that relate to the updating of the National Register of Electors. After that period and subject to the consent of the Librarian and Archivist of Canada, Elections Canada will destroy CD-ROMs, diskettes, or other physical media on which the data was provided.

Recommendation

2.65 It is recommended that Elections Canada review and update the privacy and security provisions of its information sharing agreements. It is also recommended that Elections Canada ensure that its information sharing agreements are developed and managed within a framework of modern guiding privacy principles, such as those set out in the *Guidelines for Best Practice*, referenced above.

Management Response

The Canada Elections Act provides the authority for the Chief Electoral Officer to conclude agreements for sharing the personal information of electors. The auditors found that the practice of using formal agreements for information collection and sharing exceed the requirements of the Privacy Act and the TBS policies. Elections Canada will, nonetheless, review its information collection and sharing practices taking into account modern guiding privacy and security principles.

Recommendation

2.66 It is recommended that Elections Canada obtain assurances that the data handling practices of other electoral bodies are consistent with the terms of its information sharing agreements.

Management Response

We will consult with our provincial data-sharing partners to confirm that their data handling practices are consistent with our data sharing agreements. We foresee the completion of these consultations by December 31, 2009.

Canada Revenue Agency

Introduction

3.1 As the chief administrator of federal, provincial and territorial tax laws, the Canada Revenue Agency (CRA) maintains one of the government's largest repositories of personal information. Outside of Human Resources and Social Development Canada (HRSDC), no other institution retains as much information about Canadians as the CRA. The CRA collects personal information to assess Canadian's tax obligations and to determine their eligibility for various federal and provincial economic and social benefit programs administered through the tax system. Its 'IDENT' database contains the personal information of approximately 33.4[8] million individual taxpayers.

3.2 The vast majority of taxpayers voluntarily disclose information about themselves in order to discharge their tax obligations and to qualify for the programs or benefits to which they are applying.

3.3 Given the CRA's responsibility for tax compliance and collection, it often uses sophisticated profiling, data matching and mining techniques to ensure that taxpayers are accurately stating their income and expenses. Necessarily, not all of the CRA's information gathering activities are performed with an individual's knowledge or consent. The CRA must also actively trace the whereabouts of debtors who have moved without paying tax debts.

3.4 In addition to collecting taxes, the CRA is also responsible and accountable for the collection of debts owed to programs of HRSDC, including the Canada Student Loans, Employment Insurance, Employment Programs, Canada Pension Plan and Old Age Security programs.

8 This includes some records marked as deceased for which there is ongoing tax activity.

3.5 As permitted by the provisions of section 73 of the *Privacy Act*, the Commissioner of the CRA has delegated the privacy responsibilities of the head of the institution to the Director of the Access to Information and Privacy (ATIP) division.

Why the audit is important

3.6 The CRA's data holdings are not only voluminous, they are also highly sensitive. In addition to basic identifying information (e.g., address, income, employment, SIN, marital status, children, citizenship), the CRA may, for example, collect medical data for the purpose of allowing a disability tax credit, or personal banking information for the purpose of transferring tax credits and refunds.

What we found

3.7 The CRA takes its confidentiality and security obligations very seriously. It has a strong culture of confidentiality, and comprehensive controls have been introduced over many years throughout the organization to ensure that personal information is kept secure. Sections 241 and 295 of the *Income Tax Act* and *Excise Tax Act* respectively provide a strong foundation in support of information safeguards.

Governance structure for privacy can be further strengthened

3.8 The CRA created an ATIP Oversight Committee to oversee compliance with the institution's privacy impact assessment (PIA) obligations in 2002, and to help ensure effective and timely decision-making. The Committee has Director General level representation from almost every headquarter branch (including the Security, Risk Management, and Internal Affairs directorates). It is chaired by the Access to Information and Privacy Director, who has delegated authority for the *Privacy Act* and reports to the Assistant Commissioner of the Public Affairs Branch. CRA has issued an internal PIA directive, setting out the accountabilities for the privacy impact assessment review process. The CRA recently made changes to the governance framework to include a senior level of oversight regarding privacy impact assessments. The Strategic Direction Committee, consisting of the Commissioner and several Assistant Commissioners, will review and approve all PIAs on a quarterly basis, starting in the fall of 2008.

3.9 Although the Committee's creation strengthens the organization's governance vis-à-vis privacy impact assessments, the CRA has not assigned responsibility for overseeing strategic privacy compliance activities across the organization to a senior executive or executive level committee. This is particularly important in a large institution with

significant stores of personal information, such as the CRA. There is an opportunity to further strengthen strategic privacy compliance activities.

Recommendation:

3.10 It is recommended that the Canada Revenue Agency strengthen its privacy governance structure by appointing a Chief Privacy Officer as a central locus for privacy management and for overall privacy leadership.

Management Response

CRA appreciates the importance of a strong Privacy Governance Structure and agrees with the recommendation of appointing a Chief Privacy Officer. We are undertaking the necessary steps to fulfill this initiative.

Formal collaboration between security and privacy officials is needed

3.11 CRA's Security, Risk Management and Internal Affairs Directorate is responsible for managing all matters related to the security of confidential taxpayer information.

3.12 We reviewed CRA's internal policy on managing security incidents. It sets out clear expectations for CRA's employees and managers. The policy does not, however, set out a role for CRA's ATIP Coordinator. We were advised that CRA's Security and ATIP officials collaborate informally, on an ongoing basis.

3.13 TBS' *Guidelines for Privacy Breaches* strongly recommend that an institution's Privacy Coordinator liaise and collaborate with security staff, and determine the necessity of reporting privacy breaches to the OPC. It may be difficult for the CRA's ATIP Coordinator to perform these functions without a formal mechanism in place to ensure that he or she is engaged in a review of privacy breach incidents.

Recommendation

3.14 It is recommended that the Canada Revenue Agency:

- ensure there is an information sharing protocol between the Security and Access to Information and Privacy Directorates, with respect to privacy breach reporting, and
- review and amend its guidelines and procedures on the Reporting of Security Incidents, to ensure they are consistent with those of Treasury Board Secretariat.

Management Response

CRA agrees with the importance of strengthening the collaboration between Security, Risk Management and Internal Affairs Directorate and ATIP Directorate with respect to privacy breach reporting and they will work closely together to develop a formal information sharing protocol to meet the needs of both directorates.

The Security, Risk Management and Internal Affairs Directorate will examine Treasury Board guidelines and procedures on the Reporting of Security Incidents and amend the Agency's guidelines and procedures accordingly if a need exists.

Privacy training and awareness

3.15 This past fiscal year, the Access to Information and Privacy Directorate delivered 21 ATIP awareness sessions to nearly four-hundred and fifty CRA employees across Canada. In addition, there are a large number of training courses, delivered by individual Branches of CRA, which incorporate components of confidentiality, privacy, and/or security. These topics are incorporated into CRA procedures/policy manuals and guides. This is commendable.

3.16 Besides providing training to CRA employees, the Directorate also increased the number of reference tools available online for both employees and managers. A link was added on the CRA's intranet that directs CRA officials to the "Tools and Resources Plus" page, which includes a link to ATIP. The ATIP site includes a handbook for CRA employees, annual reports to Parliament, ATIP notices, the ATIP Reference Manual, and the CRA Privacy Impact Assessment Directive and Procedures. There are also links to other ATIP-related documents such as the *Access to Information Act*, *Privacy Act*, *Info Source*, and other Treasury Board Secretariat policies.

3.17 In addition, the CRA delivered a training program specifically designed for its management group that included a module on ATIP. A total of 15 sessions were given to over 300 CRA managers in 2006/2007, meeting the Agency's objective of increasing the awareness level of CRA employees with respect to access and privacy requests.

3.18 While the Agency's training regime has been successful at providing employees with an overview of the lifecycle of a request for personal information under the *Privacy Act*, its ATIP awareness, as currently designed, falls short of providing program managers with a general awareness of core privacy principles so that they may fully consider privacy impacts when designing or implementing programs and services.

Recommendation

3.19 It is recommended that the Canada Revenue Agency expand its current ATIP awareness program to ensure all program managers receive training on generally accepted privacy principles and the TBS directive on privacy impact assessments.

Management Response

CRA recognizes the importance of expanding its ATIP awareness program across the Agency to include training that emphasizes general privacy principles and the TBS directive on privacy impact assessment. However, before we are able to establish specific goals there is a need to analyze the scope of this initiative in order for us to develop a strategic plan.

Enterprise-wide performance measures are being developed

3.20 In our 2007 government-wide audit of the privacy impact assessment (PIA) process[9], we noted that various institutions did not have processes in place to identify all activities requiring a privacy impact analysis. The absence of such a screening process – in essence, the trigger point for any privacy impact analysis – precluded institutions from properly assessing the extent of privacy risks associated with new programs and services.

3.21 Currently, CRA does not have a system to track and report on all new initiatives that might require a privacy impact assessment. As a result, it is not in a position to monitor the financial, operational, and human resource impacts of PIA operations. However, the CRA is in the process of developing a system to track ongoing initiatives. CRA is also participating in piloting the TBS' revised PIA policy instrument (still in development).

3.22 CRA's development of a system to track new initiatives, and its participation in piloting the revised PIA policy instrument, are commendable.

Information sharing agreements

3.23 CRA exchanges information with various federal, provincial, territorial and international governments. Information exchanges are generally done through specific arrangements in the form of Memoranda of Understanding (MOUs) and Letters of Intent. These formal agreements articulate the nature of the data exchange, each entity's legal authority for sharing, and the roles and responsibilities of each party with respect to the exchange. They also specify how information

9 *Assessing the Privacy Impacts of Programs, Plans, and Policies* (October, 2007), available at: www.privcom.gc.ca.

is to be exchanged, limitations on the information's use, and any security and confidentiality issues surrounding data handling. MOUs specify that internal audits are to be conducted no later than two years after the date of last signing, and that follow-up audits be conducted subsequently within timeframes agreed upon between the two parties.

3.24 Given the sensitivity and volume of data being exchanged by the CRA – not to mention the consequences associated with potential data breaches – information sharing agreements are used by management as an important means of mitigating some of the risks associated with data transfers.

3.25 CRA's practice of requiring a formal agreement with other federal institutions exceeds the requirements of the *Privacy Act*, and the current policy requirements of TBS. This is commendable, as is the CRA practice of requiring regular internal audits of the terms of its MOUs.

3.26 We reviewed the findings of eight of the CRA internal audits examining the privacy and security provisions of its MOUs with various entities. Six of the reports either assessed the security and privacy provisions of the agreements that were reviewed as adequate or made recommendations for updating/improvement, which the CRA implemented.

3.27 Two internal audit reports, one in 2005, and the follow up report in 2008, identified that the terms of the MOUs governing information sharing with HRSDC/Service Canada were out of date. The 2008 report noted that the delays were mainly a result of the numerous organizational and personnel changes within HRSDC/Service Canada.

Collection of Social Insurance Numbers of Children

3.28 A sound privacy management framework includes ensuring that the institution is only collecting information that it currently has the authority to collect, and needs. During the course of our examination we discovered that, over the past decade, the CRA has automatically collected the SINs of between six and eight million children through regular transfers of data from HRSDC/Service Canada. We asked the CRA to set out its legislative authority for the collection of the SINs of children, to identify why it needs them, and how it uses them.

3.29 The CRA's authority falls under section 248 of the *Income Tax Act* where it can collect the information for all taxpayers. A taxpayer as defined under that section is a person, whether or not that person is liable to pay tax. Since a child is a person, he or she "is also a taxpayer". Therefore, even though a child may not be a tax filer, the CRA may collect the SIN of that child.

3.30 With respect to the question of need, the CRA initially advised us that it does not currently need to use the SIN numbers of children, except in limited circumstances, such as where an income tax return is being filed on behalf of a child or for the purpose of a registered education savings plan. Since CRA's explanations were inconsistent with good privacy practice, we pursued the matter further.

3.31 CRA provided us with more information. CRA explained that it needs to have all SINs on file for all taxpayers because in addition to the use of the SIN for processing tax returns, it uses them in data matching activities to detect fraudulent use of SINs and to help prevent identity theft. The CRA provided us with information on their prevention and detection activities confirming that their policies and procedures in this area will continue to identify inappropriate uses of SINs in general, including those of children. In this way, the CRA protects the integrity of the SIN for purposes of current or future tax filing for all taxpayers.

3.32 Although there is a legal authority and a need for the CRA to collect all the SINs of children, we are concerned that the CRA did not formally address such questions and consider the potential privacy risks and impacts of automatically collecting children's SINs at birth. This issue should have been explicitly addressed and decisions documented as part of a robust privacy management framework.

Recommendation

3.33 It is recommended that the Canada Revenue Agency establish a policy and plan for managing the Social Insurance Numbers of children.

Management Response

For the entire SIN database maintained by the CRA, the Agency has an established policy for SIN management. This policy is reviewed periodically and it is part of the identity renewal initiative – a multi-year project began in 2006 to renew all aspects of its IDENT database. The Agency will review existing policies and procedures with a view toward enhancing the secure treatment of the SINs of children.

Human Resources and Social Development Canada (HRSDC) including Service Canada

Introduction

4.1 Human Resources and Social Development Canada/Service Canada is responsible for developing, managing and delivering programs and services that provide Canadians with income support, labour market information and skills development opportunities, and other tools intended to help Canadians to thrive economically and socially. HRSDC has extensive personal information holdings in support of its many programs. Further information is available through *Info Source*, which details sources of information for all federal institutions.

4.2 HRSDC's Report on Plans and Priorities (RPP) for 2008-2009 indicates planned expenditures on programs and services of more than $87 billion. Taken together, HRSDC and Service Canada have some 23,500 full-time employees.

4.3 HRSDC was created on February 6, 2006 by regrouping the former Human Resources and Skills Development Canada and Social Development Canada. Those two institutions had been formed just over two years earlier, in December 2003, by splitting Human Resources Development Canada into two separate institutions which, however, continued to share many common services and operations. The new institution also encompasses the Service Canada initiative, launched in 2005.

4.4 HRSDC focuses on policy and program design and research, while its operating arm, Service Canada, undertakes delivery functions.

4.5 Service Canada manages the Social Insurance Register, the central repository of Social Insurance Numbers (SINs) established under the provisions of the *Employment Insurance Act*, in 1964. The SIN was originally intended to serve as a client account number for Canadians in receipt of Canada Pension Plan and Old Age Security benefits, and employment support programs. It subsequently became a file identifier for income tax purposes. Canadian citizens, permanent residents and temporary residents with a valid authorization to work in Canada are eligible to receive a SIN.

4.6 The Social Insurance Register (SIR) contains an individual's name, date of birth, assigned SIN, place of birth, and parents' names. Death dates are also recorded in the SIR, which contains almost 31 million active records.

4.7 Under the provisions of section 139 of the *Employment Insurance Act*, Service Canada is authorized to issue SINs. A growing number of parents are requesting a SIN in order to establish an education savings program for a child (a program where the SIN of the child is

required), to establish an interest-bearing savings account, or simply because they find it convenient to request a SIN for their child at birth. As a result, the SIR contains the SIN numbers and personal information of millions of children whose parents have chosen to apply for a SIN on their behalf.

4.8 Each of Service Canada and HRSDC has had a Chief Privacy Officer, and a dedicated Access to Information and Privacy (ATIP) Directorate. As of July, 2008, the two existing ATIP Directorates have been combined under the leadership of one ATIP Director for HRSDC/Service Canada. As well, the Corporate Secretary for HRSDC is now the Chief Privacy Officer. The position provides strategic leadership and oversight of privacy compliance activities for all of HRSDC, including Service Canada.

Why the audit is important

4.9 The SIN is a key piece of personal information that can be used, along with other personal information, to steal an individual's identity. It can also be used to match information in other databases, and develop data profiles, potentially threatening an individual's privacy rights.

4.10 Service Canada provides citizens with a one-stop window to government services and information in over 300 points of service across the country. Its 19,000 employees, particularly those working in front-line service, deliver a growing number of services and benefits on behalf of HRSDC and on behalf of other federal institutions. In addition to the SIN, its employees are collecting, using and sharing other very sensitive information, for example, the credit card number of Canadians who pay a fee for a service, such as the processing of a passport application, at a Service Canada counter.

4.11 Absent an appropriate privacy management framework, there is a significant risk that the personal information and privacy rights of Canadians may not be assured.

What we found

4.12 While HRSDC/Service Canada has a robust privacy management framework, it needs to be revitalized and used to its full potential.

The Privacy Management Framework needs to be revitalized

4.13 Human Resource Development Canada (the predecessor department of HRSDC/Service Canada) first developed and approved an overarching framework for privacy, a "Privacy Management Framework" (PMF) in 2001. The PMF has four "pillars": strategic planning and governance, risk management, cultural change, and assurance of compliance. Each pillar has its associated high level goals and/or describes fundamental privacy principles that the institution

has embraced. The PMF describes privacy as a "fundamental right of Canadians", "a shared responsibility", and "an element of recruitment, promotion and performance management". Its impact, for the institution, means a shift "from a reactive, issues driven posture, to a strategic and proactive stance".

4.14 The HRSDC Senior Management Committee approved enterprise-wide accountabilities for Privacy and Security on September 3, 2004. The decision was based on the accountabilities described in a presentation document prepared as part of the enterprise-wide Privacy Management Framework. With the transformation of HRSDC into its successor institution and with the implementation of Service Canada, the PMF of HRSDC was extended into the management and accountability framework of the new entity and as well into the Service Canada organization.

4.15 Enterprise-wide committees were created as part of the governance instruments of the PMF approved in 2004. There were three senior-level committees to collaborate on overlapping privacy responsibilities: the Privacy Management Framework Steering Committee (PMFSC), the Databank Review Committee, and the IT Security Governance Committee.

4.16 The PMFSC was to be pre-eminent amongst the three committees: it was to "direct the enterprise-wide implementation of the Privacy Management Framework". It was also charged with identifying "enterprise-wide privacy priorities and establish(ing) timelines." The Databank Review Committee was to "review all policy analysis, research and evaluation activities that involve the use of unmasked personal identifiers or the linking of personal information databanks." The IT Security Governance Committee was to "direct the enterprise-wide IT Security function", examine cross jurisdictional IT Security issues, and act as the accreditation authority for the Department's IT systems, applications and services. The recommendations of all three committees would go to the Deputy Minister of HRSDC for review and approval.

4.17 In our view, the Committees as structured provide a strong and integrated privacy governance regime. However, the Committee structure has lost some of its desirable attributes and functions, leading to a weakening of the framework, with the potential for unforeseen results. We identified several indicators of this weakness.

4.18 The Committees do not share the minutes of each others' meetings and decisions. The PMFSC is therefore hampered in fulfilling its role as the pre-eminent institutional privacy management committee.

4.19 The PMFSC has had relatively lower level representation from the branches of the institution over the last few years, as indicated by the minutes of meetings. Originally the Director General from a program

group chaired the Committee. This had not happened in a consistent fashion for two years (2006-2008). As of May of 2008, an Assistant Deputy Minister of Service Canada and the Corporate Secretary of HRSDC chair the committee.

4.20 We learned that the stated 2004/2005 goals of the PMFSC are only now being updated.

4.21 It is unclear if PMFSC has been dealing with all aspects of privacy governance and management as intended. There is no indication that the PMFSC was in a position, as shown by the agenda of meetings, that it could effectively deal with two of the four "pillars" of the privacy management framework, i.e. risk management, and assurance of compliance. The issue of risk management was examined only for new or changed programs. We recognize that HRSDC/Service Canada has been addressing cultural change to some extent, with its work on privacy-related education and training. However, more attention is needed to other aspects of cultural change, such as implementing a communication plan for privacy and visibly building privacy principles into strategic planning processes.

4.22 Clearly, the PMFSC has a potentially strong oversight role with respect to privacy impact assessments. However, there is no indication that the PMFSC reviews the risk management or privacy compliance of existing programs and activities on a regular basis. The Committee could have done this by reviewing the results of the periodic privacy program monitoring undertaken by HRSDC's branches, and by reviewing the corrective actions taken by management as a result of internal audit reports related to privacy.

4.23 We are aware, for example, of two internal reports with a significant impact on privacy that could have been discussed and reviewed by this Committee, but were not. The first is the 2004 HRSDC Internal Audit of Personal Information. The second is the Independent Review of the Integrity of the SIN and SIR of November 2006.

4.24 Other committees at HRSDC and Service Canada also deal with privacy issues. For example, the HRSDC Management Audit and Evaluation Committee received an update on management corrective actions taken with respect to the 2004 Internal Audit of Personal Information in January 2008. This was limited, however, to 3 of 14 recommendations deemed applicable to the HRSDC component of the audit. The Service Canada Audit Committee was not provided with an update at the time of the audit on actions taken on the remaining 11 recommendations[10].

10 In May, 2008, the audit committees of HRSDC and Service Canada were combined.

4.25 We were advised that the Deputy Head Senior Staff Committee and the Service Canada Management Board also consider privacy issues on a regular basis. However, these committees are not mandated to assess privacy impact assessments in detail.

4.26 As originally designed, the PMFSC was to play the key role in the integration and management of privacy related information at the corporate level. If it is to function in that role, there needs to be a mechanism whereby privacy related information is shared with the PMFSC by other corporate committees on a timely basis.

4.27 We also determined that the IT Security Governance Committee has not convened a meeting since 2006. The IT Security Governance Committee's mandate was to consider the potential impact on privacy of major systems changes. The Committee is, in effect, non-functional. This has the potential to have major negative impacts for the protection of privacy. Departmental policy requires that a PIA should be undertaken "if the project involves significant changes to the business processes or systems that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information." It is not clear that the PMFSC is being made aware of potential systems changes through the privacy impact assessment process.

4.28 To provide a strong and integrated privacy governance regime, the PMFSC needs to be able to deal more effectively with all four "pillars" of the privacy management framework, including the assurance of compliance and performance management.

Recommendation

4.29 It is recommended that HRSDC/Service Canada revitalize the role of the Privacy Management Framework Steering Committee (PMFSC).

Management Response

The department understands the importance of the role of the Privacy Management Framework Steering Committee. Membership in the Committee has been updated and confirmed at the Director-General level. The Chief Privacy Officer and the ADM of Policy, Partnerships and Corporate Affairs serve as co-chairs of the Committee.

The Privacy Management Framework Steering Committee will comprehensively address privacy governance within its mandate and is discussing options for further revitalization of the Committee. The Committee is updating its work plan and is also focusing on institution-wide privacy issues and actions, including consideration of all four pillars of the Privacy Management Framework.

Privacy is everybody's business

4.30 The privacy responsibilities of staff, managers, the Chief Privacy Officer(s), and senior executives are set out in the HRSDC Departmental Privacy Policy, available on the HRSDC and Service Canada intranet sites.

4.31 The privacy accountabilities of program ADMs include:

- design Branch frameworks, including business processes, that comply with the *Privacy Act* and other applicable privacy protection laws, and
- identification of personal information required to administer the programs and activities under their authority.

4.32 Prior to the amalgamation of the privacy functions in July 2008, both HRSDC and Service Canada had designated Chief Privacy Officers (CPO), at the ADM level and both HRDSC and Service Canada each had a director of Access to Information and Privacy (ATIP). These functions were recently merged into one. There are eight regional privacy coordinators for the institution. The ATIP organizations for HRSDC and for Service Canada are well publicized on their intranets and referenced in the internal privacy codes and privacy policies and guidelines.

4.33 HRSDC/Service Canada has advised that its Annual Report on Privacy for HRSDC/SC for 2007-08 indicates that HRSDC's Access to Information and Privacy Directorate provided 36 training sessions to 565 employees within the Department. Similarly, the Access to Information and Privacy, Privacy Policy and Human Rights Division at Service Canada provided training to 475 Service Canada employees on the requirements of the *Act*. A total of 24 sessions were provided in regional offices and at National Headquarters and included sessions for senior management. In addition, Access to Information and Privacy training was given at the "Orientation for New Employees" sessions for both HRSDC and Service Canada.

4.34 In the National Capital Region, Service Canada operates its own training site, the Service Canada College. It provides all new employees of HRSDC/Service Canada with a mandatory introductory training program on privacy and information security. Employees in the regions are provided with on-site face-to-face training on the privacy policies.

4.35 A three hour session training employees on the appropriate safeguards to use with mobile devices, entitled "removable information security protection", has recently been delivered three times. It will be a permanent offering of the Service Canada College.

4.36 Service Canada provides certification for front-line agents that pass the mandatory SIN-issuance training. HRSDC/Service Canada indicates that as of June, 2008, 2,344 employees have received this certification. Moreover, agents who have not processed SIN requests for a period of 120 days are subject to recertification.

4.37 The Departmental Privacy Policy and the associated Privacy Guidelines are detailed and comprehensive. There is a logo that says "privacy is everybody's business". We agree, especially since the programs delivered to Canadians by HRSDC and Service Canada touch almost all Canadians over a period of time. In our view, the Departmental Privacy Policy and the associated Privacy Guidelines should be widely shared with all Canadians.

Recommendation

4.38 It is recommended that HRSDC/Service Canada publish its Departmental Privacy Policy and the associated Privacy Guidelines on the department's website, making them available to Canadians who have access to the internet.

Management Response

We are committed to reviewing, updating and posting the Departmental Privacy Policy and associated Privacy Guidelines on each of the Departmental Internet sites. The published versions will also reference the new Treasury Board Policy on Privacy Protection instituted in April, 2008.

Enterprise-wide program delivery coordination and risk management mechanisms are in place or in development

4.39 As indicated previously, HRSDC approved enterprise-wide accountabilities for privacy and security in September, 2004. The accountabilities of Deputy Ministers, Branch ADMs, Regional Executive Heads, Managers, and individual employees, Chief Privacy Officers, Departmental Privacy Coordinators, and Regional Privacy Coordinators, Chief Security Officers, Departmental Security Officers, and Regional Security Officers are documented in detail. The accountabilities specifically identify privacy impact assessments as a key risk management tool.

4.40 The Privacy Management Framework Steering Committee (PMFSC) has in its terms of reference a requirement that privacy impact assessments be conducted for all new initiatives so as to "address the ongoing development of new programs and the redevelopment of existing ones".

4.41 Third party service providers that collect personal information on behalf of HRSDC are bound by contractual clauses that address their

privacy obligations. They also receive directives on the management of personal information to enable them to understand and apply the institution's privacy policy. A document entitled: "Model Privacy Clauses for Use in Contracts" is available on the HRSDC intranet site.

Better control of Information sharing agreements needed

4.42 The HRSDC/Service Canada *Guidelines on Information Sharing Agreements* were released as a "Final Draft" on October 23, 2007. The guidelines require that Programs/Regions draft Information Sharing Agreements (referred to either as ISAs or Memoranda of Understanding (MOUs)) in consultation with Legal Services and the respective ATIP Directorates. A Privacy Impact Assessment (PIA) Checklist is to be completed to determine whether a PIA is necessary.

4.43 The guidelines indicate that the "ATIP Directorate is responsible for maintaining a current inventory of ISAs for HRSDC/ServCan" and the listings are "periodically updated with input from the Program/ Region". We were unable to obtain the number of ISAs / MOUs in effect at the time of this audit.

4.44 HRSDC/Service Canada provides unofficial templates to draw up MOUs regarding data collection and sharing for proposed agreements. However, we were unable to determine to what extent ISAs / MOUs are updated to reflect Service Canada's Privacy Code, program changes, and the most current provisions of applicable legislation.

4.45 We understand that Service Canada has information sharing agreements governing most exchanges of personal information that occur with federal institutions, and provincial and territorial governments with which it exchanges information. However, absent an up to date inventory, it is not possible to confirm this claim.

Recommendation:

4.46 To better manage its information sharing agreements, it is recommended that HRSDC/Service Canada update and maintain an inventory of its information sharing agreements, and develop a schedule for their review and renewal.

Management Response

Information sharing agreements are an important way to ensure personal information is handled according to sound privacy principles. The department is committed to reviewing its information sharing agreements and will develop a methodology for updating agreements. It will also develop a comprehensive inventory of all agreements involving the use and disclosure of personal information.

Guidelines, policy and procedures exist to protect the integrity of the information held in the SIR

4.47 Both the *Department of Human Resources and Skills Development Act* and the *Department of Social Development Act* contain privacy provisions with specific penalties for unauthorized or inappropriate access, use or disclosure of personal information.

4.48 The Departmental Security Policy and Procedures Manual has set procedures for the collecting and handling of sensitive information. It covers access requests, off-site transport and storage security practices for workstations, LAN and electronic mail security and Telework security.

4.49 The Departmental guidelines regarding the SIN program specify that personal information contained in the SIR is confidential and should, under no circumstances, be disclosed to third parties. The guidelines on the Service Canada intranet explain that "The use of SIN information is governed by the *Privacy Act* and the *Employment Insurance Act*. Access to SIR Online is controlled to protect the integrity of the data and the disclosure of highly confidential information."

4.50 According to HRSDC, the Integrity Services Branch plays the lead role in implementing an enterprise-wide Operational Risk Management approach. It includes activities to prevent, deter and detect abuse and fraud against the Employment Insurance, Canada Pension Plan and Old Age Security programs, and to manage program integrity risk responses at the regional and national levels. In addition, integrity activities are aimed at reducing errors, omissions, fraud and abuse across the benefits and services delivered by Service Canada, through the use of new tools, including pattern analysis, flagging and data, statistical and trends analyses.

Process for managing privacy breaches is in place

4.51 TBS has issued *Guidelines for Privacy Breaches*, to help institutions to avoid instances of improper or unauthorized access to or disclosure of personal information, and to mitigate the consequences of a breach, should one occur. The *Guidelines* recommend that more serious privacy breaches be reported to the OPC.

4.52 Our interviews with HRSDC/Service Canada senior managers suggest that the Department takes privacy breaches very seriously, implementing preventive actions to prevent recurrences, where appropriate. Privacy breaches are reported to the OPC, depending on the potential impact and scope of the breach.

4.53 The Integrity Services Branch of Service Canada oversees the risk management process for privacy and security matters. As of the fall of

2007, it receives all reports of privacy breaches, and their handling is managed by the Assistant Deputy Minister of this Branch.

Treasury Board Secretariat

5.1 Treasury Board Secretariat (TBS), a central agency of the federal government, is obligated under the *Privacy Act* to prepare and distribute directives and guidelines concerning the operation of the *Act*. It has complete discretion as to how and to what extent it fulfils this obligation.

5.2 In 1997, the Prime Minister of Canada conferred upon the Treasury Board, a Cabinet committee of the Queen's Privy Council for Canada, and its administrative arm, the Treasury Board Secretariat (TBS), an enhanced role as the government's management board, with the mandate to support institutions in improving their administrative and managerial practices.

5.3 In 2000, TBS released *Results for Canadians: A Management Framework for the Government of Canada*, which set out a vision for modernizing the public service. The report calls for more citizen-centered delivery of services, and a series of government-wide policies and processes to promote better decision-making, greater accountability and a more modern approach to risk management.

5.4 While it has no direct responsibility for ensuring that institutions comply with the *Privacy Act,* TBS is accountable to the Government of Canada, and a representative frequently appears before the Standing Committee on Access to Information, Privacy and Ethics. The President of the Treasury Board, as designated Minister for the *Act* and as a member of Cabinet, is responsible to the House of Commons and is often asked to respond to questions on behalf of the government on privacy policy issues. In our view, in the collective, TBS and federal institutions share a responsibility for ensuring compliance with the *Act* and good privacy practices.

5.5 TBS regularly issues Implementation Reports and Information Notices to the Access to information and Privacy (ATIP) community to address emerging questions that are interdepartmental in scope, including changes to policy requirements or to the interpretation of the legislation. These are intended to play a key role in supporting sound privacy management practices within federal government institutions.

5.6 TBS has issued various policies, directives and guidelines setting out expectations regarding the management of the privacy and security of personal information. These include, for example, the *Policy on Privacy*

Protection (2008), the *Government Security Policy (2002)*, the *Privacy Impact Assessment* (PIA) *Policy (2002), Guidelines for Privacy Breaches (2003)*, and the *Directive on the Social Insurance Number (2008)*. TBS policies and directives, while ensuring compliance with the *Act*, set a higher standard. They reflect modern privacy principles, which emphasize the right of the individual to control the collection, use and disclosure of his or her personal information.

5.7 In 2003, TBS introduced the Management Accountability Framework (MAF), which sets out its expectations for good management of an institution. It is organized around ten key elements. TBS has developed performance indicators associated with each of the elements, and administers a compliance assessment annually to selected institutions. In 2006, personal information management was added as a MAF area of assessment. TBS advised us that MAF results may not necessarily reflect actual performance with respect to the *Act*.

5.8 The indicators that TBS has used to determine if an entity subject to MAF is complying with its privacy obligations have been adapted annually. In its most recent round of assessments, TBS looked at the public accountability tools of 46 selected institutions: their Annual Reports to Parliament, their Reports on Plans and Priorities, their Departmental Performance Reports, and their entries in *Info Source*, the federal compendium that describes the personal information bank holdings of organizations subject to the *Act*.

5.9 TBS did not rate accountability for privacy as strong for any of the 46 institutions that it recently reviewed. Fourteen were rated as adequate, 31 were rated as needing improvement, and one was rated as not nearly adequate. This is a disappointing result. TBS has advised us that it is providing support to the ATIP community to address the MAF results.

5.10 At the same time, the MAF is only applicable to the heads of institutions identified in a Schedule to the *Financial Administration Act*. This is a universe of approximately 100 entities. The MAF does not apply to approximately 150 other institutions that are subject to the *Act*.

5.11 TBS has recently advised that for entities not subject to the MAF, it intends to address issues of governance, risk management, training and awareness, program monitoring and reporting, and administration of the *Privacy and Access to Information Acts*, in the context of its review and renewal of privacy policies. Such an initiative is welcome and needed.

5.12 In addition to its ongoing policy work, TBS has:

- enhanced the reporting requirements set out in section 72 of the *Act*. (These state that the head of every government institution

must prepare an annual report on its administration of the *Act*, for submission to Parliament). Heads must report comprehensively on a broader spectrum of privacy management responsibilities;

- issued a report entitled '*Guidance Document: Taking Privacy Into Account Before Making Contracting Decisions*', that contains a detailed risk assessment of contracting (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_e.asp). The document is intended to guide federal institutions that enter into third party agreements for service, and to address concerns regarding the implications of the *USA Patriot Act*, and the transborder flows of personal information.
- issued 'Privacy Matters', a report that provides a synopsis of the impact of the *Patriot Act* on the privacy of Canadians.
- Assisted in the development of *Government-to-Government Information Sharing Agreements – Guidelines for Best Practice*.
- issued *Guidelines for privacy breaches*.

5.13 The OPC is precluded, under a strict reading of the *Privacy Act*, from independently assessing the role of TBS in its capacity as a central manager for privacy. Nevertheless, we are aware of several important gaps that TBS recognizes it needs to address. These include:

- issuing directives to implement recently revised privacy policies,
- Implementing a new policy on privacy impact assessments,
- developing policy and guidance on identification and authentication,
- leading the development and promotion of a core privacy training curriculum for government employees,
- establishing effective guidance on the sharing of personal information between federal institutions, and between levels of government, and
- creating a model privacy management framework for institutions.

5.14 Meeting these needs will enhance TBS' leadership and strengthen the overall privacy management of the federal government.

Comments of the Treasury Board Secretariat

Policies and Directives

On April 1, 2008, TBS issued the Directive on the Use of the Social Insurance Number (SIN) and a new Policy on Privacy Protection. As part of its ongoing policy suite renewal exercise, TBS also intends to issue the following three directives on April 1, 2009: the Directive on Privacy Practices, the Directive on Privacy Impact Assessments, and the Directive on Requests for Access and Correction of Personal Information. The Secretariat will also develop supporting guidance documents and tools to further assist institutions and further strengthen their privacy management practices.

In addition, in the fall of 2008, TBS intends to issue a new Policy on Government Security and a related new Directive on Identity, which will include direction and guidance on identification and authorization.

A core privacy training curriculum

For the past several years, TBS has been providing training to the Access to Information and Privacy (ATIP) Community. TBS holds bi-monthly community meetings, annual conferences and weekly workshops on Access of Information and Privacy including sessions on Personal Information, Fair Information Practices and Privacy Impact Assessments. This is in addition to ongoing advice given by TBS to individual institutions (both to ATIP and other program officials) on specific issues of interest to them.

In 2006, the Federal Accountability Act brought a number of important changes to both the Access to Information Act and the Privacy Act. One of the changes that affected the ATIP Community was the expanded coverage of the Acts from some 186 government institutions to approximately 250. With this in mind, TBS has recently concluded a survey of ATIP professionals designed to better understand and assess the current and future needs of the community. In response to some of the preliminary findings of the survey results, TBS is working with both the Canada Public Service Agency (CPSA) and its own Organizational Readiness Office to explore options for greater capacity building. In addition, TBS is collaborating with the Canada School of Public Service (CSPS) to develop a curriculum on privacy awareness and privacy responsibilities of government employees.

TBS also intends to continue to explore further means to enhance training and developmental opportunities for ATIP practitioners as well as to strengthen privacy management in the public service in general.

Information sharing Agreements

TBS guidelines currently include guidance on information sharing agreements and practices both in the context of disclosures under the Privacy Act and data matching activities. The guidelines also include information about the components of information sharing agreements. In addition, TBS provides significant advice and assistance to institutions in that regard, as part of its ongoing review of individual Personal Information Banks and daily telephone and email inquiries. Moreover, as an active member of the Privacy Subcommittee of the Public Sector Chief Information Officer Council, Treasury Board Secretariat assisted in the development of the Personal Information Sharing Agreement Guidelines, intended for the use of all jurisdictions within Canada. TBS officials presented these guidelines to the federal Access to Information and Privacy

(ATIP) Community in 2007, and recommended that they be used as an initial model in conjunction with Privacy Act requirements.

In 2006, TBS also committed to develop new guidelines on Information Sharing Agreements (ISAs) for the intended use of federal institutions subject to the Privacy Act. These guidelines are currently in draft format and are the subject of consultations with affected stakeholders. TBS intends to issue the Information Sharing Guidelines to ATIP Coordinators and publish them on its website by the end of the 2008/2009 fiscal year.

Model privacy management framework for departments

The Policy on Privacy Protection (April, 2008), established the basis for the ongoing policy work which is aimed at defining and structuring a sound privacy management strategy that can be integrated within government institutions. Once the privacy policy suite renewal is finalized, the policy, directives and guidelines will promote the key elements of an effective privacy management framework which consists of having in place sound governance, ongoing risk management, effective administration, active monitoring and reporting as well as integrated training and awareness with respect to the Privacy Act. In line with the TBS consultations carried out prior to finalizing the policy, officials of the Office of the Privacy Commissioner, as well as all other federal institutions that fall under the jurisdiction of the Privacy Act, will be consulted on other policy instruments and any tools or models that are developed in support of the policy.

Conclusion

6.0 As the foregoing observations and recommendations illustrate, there are significant opportunities to strengthen the privacy management frameworks of federal institutions in order to assure Canadians that their privacy rights are fully served.

Audit team

Director General: Trevor R. Shaw

Raymond D'Aoust, Assistant Privacy Commissioner

Audit lead: Kie Delgaty

Subhas Roy

Stephen Ayres

Ned Eustace

Navroze Austin

Paul Zind

APPENDIX A

Audit Objectives and Criteria[11]

AUDIT OBJECTIVES:

A: To determine whether selected federal government institutions that collect, use, retain, and disclose personal information have implemented elements of a sound privacy management framework, with respect to the creation and control of major databases.

A sound privacy management framework will be demonstrated if selected federal institutions have:

1. an effective governance and accountability framework
    1. Roles and responsibilities for the handling and management of personal information are defined and assigned, communicated throughout the organization, and incorporated into the institution's control regime
    2. An individual/body of senior personnel oversees compliance with the institution's privacy obligations, and ensures effective and timely decision making with respect to privacy outputs (such as PIAs)
2. enterprise-wide privacy program delivery standards, program delivery coordination and risk management mechanisms
    1. the responsibilities and accountabilities of privacy and departmental security staff are coordinated and collaborative
    2. there is an effective interface between regional and corporate operations to ensure that the front end delivery of services meets clearly articulated privacy standards, and reflects best practices with respect to obtaining individual consent
3. systems and practices in place to ensure effective compliance and performance monitoring
    1. The institution establishes annual and multi-year privacy performance plans, targets, and measures, and reports on results
    2. It monitors, assesses and adapts its privacy policies, procedures and practices on an ongoing and as-needed basis
    3. It assigns resources and evaluates delivery options to ensure that it can effectively and efficiently discharge its obligations under the GoC privacy regime

11 These audit objectives and criteria were used for our review of the Privacy Management Frameworks of the Canada Revenue Agency, Elections Canada, and HRSDC/Service Canada.

Audit Objective A: To determine whether selected federal government institutions that collect, use, retain, and disclose personal information have implemented elements of a sound privacy management framework, with respect to the creation and control of major databases.

Line of Inquiry # 1:

A sound privacy management framework will be demonstrated if selected federal institutions have an effective governance and accountability framework:

1. Roles and responsibilities for the handling and management of personal information are defined and assigned, communicated throughout the organization, and incorporated into the institution's control regime, and
2. An individual/body of senior personnel oversees compliance with the institution's privacy obligations, and ensures effective and timely decision making with respect to privacy outputs (such as PIAs).

Criteria and Source	Audit Questions	Information Required and Source
We expect federal institutions to • Define roles and assign responsibilities for privacy policy development and privacy compliance throughout the organization • Establish mechanisms to ensure senior level compliance monitoring • Implement practices that ensure continuous learning, performance improvement, and timely decision making	Has the institution set out a privacy management framework that identifies the positions within the organization that are responsible for privacy practice, and their respective areas of accountability and authority? Is the framework communicated through the organization? Are the responsibilities of staff incorporated into the institution's performance appraisal/ management framework? Are learning and training plans consistent with the privacy responsibilities of each position? Is there a body or committee of senior personnel, representing a cross-section of the organization, to oversee privacy compliance activities? If accountability is vested in an individual, does s/he have the authority and accountability to achieve results? Is there a process in place to ensure timely decision making regarding program design and delivery practices that affect privacy? Are there regular and ongoing training sessions on the PIA policy, and on the administration of and compliance with the Privacy Act?	Performance appraisal/management framework/policy and activities Staff learning plans/Job descriptions Terms of Reference of Senior Management (Privacy) Committee Minutes of meetings and decisions taken Curricula for staff training programs and reports on staff training activities Departmental Performance/Annual Reports IT plans for upcoming initiatives (significant changes to architecture and process) <u>Sources:</u> Past OPC audits and reviews of PIAs Discussions with institution management – Privacy Committee members, Privacy Coordinators, IT and corporate services, program delivery managers and staff

Audit Objective A: To determine whether selected federal government institutions that collect, use, retain, and disclose personal information have implemented elements of a sound privacy management framework, with respect to the creation and control of major databases.

Line of Inquiry #2

A sound privacy management framework will be demonstrated if selected federal institutions have enterprise-wide program delivery coordination and risk management mechanisms:

1. the responsibilities and accountabilities of privacy and departmental security staff are coordinated and collaborative, and
2. there is an effective interface between regional and corporate operations to ensure that the front end delivery of services meets clearly articulated privacy standards, and reflects best practices with respect to individual consent.

Criteria and Source	Audit Questions	Information Required and Source
We expect Federal institutions to • develop and regularly review privacy policies that identify the institution's purposes for collecting, using, retaining and disclosing personal information • obtain meaningful consent for its proposed practices • limit collection, use and disclosure of personal information to the identified and legitimate purposes for which consent has been obtained	Do those responsible for privacy practice in the institution collaborate with departmental security staff, regional operations management and staff, and other key stakeholders to ensure effective program delivery and coordinated risk management? Are privacy policies citizen-centred, adapted to the institution's programs, reviewed regularly, and made available at the time the institution collects personal information? Do those responsible for privacy practice participate in and/or lead cross jurisdictional and horizontal privacy initiatives? Is a system in place to effectively report all new initiatives that may require a PIA/PPIA? Are memoranda of understanding for the sharing of personal information current and comprehensive?	Privacy policies/brochures, web pages DSO and PO job descriptions, reports on initiatives Departmental Directives MOUs re: Data sharing agreements Existing audit of PIA practices Minutes of meetings with privacy and departmental security representation Review of privacy policy language OAG work

Audit Objective A: To determine whether selected federal government institutions that collect, use, retain, and disclose personal information have implemented elements of a sound privacy management framework, with respect to the creation and control of major databases.

Line of Inquiry #3

A sound privacy management framework will be demonstrated if selected federal institutions have systems and practices in place to ensure continuous and effective compliance monitoring:

1. The institution establishes annual and multi-year privacy program delivery standards, targets, and measures, and reports on results,
2. It monitors, assesses and adapts its privacy policies, procedures and practices on an ongoing and as-needed basis, and
3. It assigns resources and evaluates delivery options to ensure that it can effectively and efficiently discharge its obligations under the GoC privacy compliance regime

Criteria and Source	Audit Questions	Information Required and Source
We expect federal institutions to • establish institution wide quality and performance standards with respect to: 1. the integrity/accuracy of the personal information holdings, 2. safeguards and access, 3. the notification requirements and risk mitigation measures for privacy breaches, and monitor their achievement. • ensure that any contracted third parties deliver services according to clearly articulated quality standards • establish and monitor a complaints handling and resolution process that includes performance improvement targets, as appropriate	Is there a reliable and comprehensive system for capturing privacy complaints and privacy breaches, to ensure that they are identified, reported and remedied? Are the results of privacy risk assessments reported (for example, in Annual Reports)? Does the regular performance monitoring include means such as automated identification and reporting of unusual IT transactions, the analysis of system use patterns, and internal privacy audits? Are performance standards set, measured, and monitored? Are quality improvement measures set? Are best practices in privacy implemented?	Best practice fact sheets Policy on reporting of privacy breaches Policy on handling privacy complaints IT measures/tools and reports that track system usage patterns Departmental Reports on Plans and Priorities Departmental Annual Reports Internal audit reports and program evaluations

Appendix B

Passport Canada

B.1 In October 2006, the OPC initiated an audit to assess the extent of Passport Canada's compliance with its *Privacy Act* obligations separate from, and prior to, undertaking the concurrent audit with the Office of the Auditor General. The OPC audit of passport operations was reported in full in the Privacy Commissioner's most recent Annual Report under the *Privacy Act.* The complete report, available at: www.privcom.gc.ca, contains a total of 15 recommendations, many of them directed at improving the security of Passport Canada's records retention and disposal practices, the physical layout of facilities, and the integrity and handling of personal information in Canada and missions abroad where passport applications are processed. The paragraphs below provide only a synopsis of the key findings that specifically relate to the privacy management framework of Passport Canada. In this case, the observations made here are effective as of January 31, 2008, when the examination was completed in this separate audit.

B.2 The recommendations arising from the audit have not been reproduced here. The Department of Foreign Affairs and international Trade and Passport Canada have already responded to the OPC's recommendations in the separate audit. The observations made in that audit have been drawn upon in reaching the overall conclusion of the audit of Privacy Management Frameworks.

Introduction

B.3 Passport Canada has more than 3,000 employees providing services at 33 locations across Canada. It also has contracts with Canada Post and Service Canada to provide over the counter passport receiving services at more than 150 locations. The agents at these locations ensure the passport applications are complete, and collect the passport processing fee.

B.4 Passport Canada and the Consular Services and Emergency Management Branch (Consular Services) of the Department of Foreign Affairs and International Trade (DFAIT) also coordinate the overseas delivery of passport and emergency travel document services to Canadians through 139 Canadian missions and more than 100 Honorary Consul offices.

B.5 Passport Canada's Integrated Retrieval Information System (IRIS) is an electronic passport issuing system used to manage the passport entitlement and production process. As of January, 2008, it contained more than 17 million active records. Passport Canada stores passport related data for up to 100 years in two databases, containing more than 30 million records.

B.6 As permitted by the provisions of section 73 of the *Privacy Act*, the Deputy Minister of DFAIT has delegated the privacy responsibilities of the head of the institution to the Director of the Access to Information and Privacy (ATIP) division at DFAIT, for DFAIT and Passport operations. The delegation has not been given to Passport Canada.

Why the audit is important

B.7 As with other institutions, Passport Canada, its receiving agents, and the Consular Services of DFAIT collect foundation identity documents such as original birth certificates, driver's licences or provincial health cards, as well as phone numbers, and credit card information. Passport Canada retains information about the name, date and place of birth, citizenship, address, assigned passport number, marital status, and gender of passport applicants. Unauthorized or inappropriate access to this information could place Canadians at risk of identity theft and/or fraud.

What we found

B.8 Passport Canada is dedicated to high quality customer service and to the integrity of a Canadian passport.

B.9 Several commendable privacy practices were identified. For example, Passport Canada began a privacy training program for its operational staff and management as of December 2007. We found the privacy training material to be comprehensive.

B.10 On the whole, however, weaknesses identified collectively pose appreciable risk to the privacy rights of Canadians. Had a stronger framework been in place, we believe various issues would have been better managed.

Governance structure and accountability measures need to be strengthened

B.11 The passport program is complex, handles very high volumes of sensitive information, and has privacy challenges and needs. We identified gaps in the coordination and implementation of privacy responsibilities. Passport Canada needs a privacy "champion" at the corporate decision-making table, and should consider appointing a Chief Privacy Officer.

Coordinated Privacy and Security awareness training needs to continue

B.12 While most of the staff interviewed during the audit of passport operations were aware of the confidentiality provisions of the *Privacy Act*, a majority could not recall having received privacy or information security training. There were other gaps in their knowledge of important privacy issues. DFAIT employees at diplomatic missions that were visited during the audit were not aware of their level of security clearance, and did not understand the security risks and internal policies governing the use of electronic devices such as cell phones, memory sticks, and blackberries.

B.13 The ATIP directorate and security officials at DFAIT have been delivering security and privacy awareness training for a number of years to diplomats and consular officials leaving for postings overseas. However, as most locally engaged staff do not have the opportunity to travel to Canada, it is a challenge for DFAIT to provide them with in-person privacy and security training.

Privacy risks in ongoing operations and in new initiatives need to be addressed

B.14 Passport Canada has a policy and operating procedures for handling and reporting security incidents. The policy applies to all facilities at headquarters and at regional offices. However, it does not have a protocol for the systematic reporting of privacy breaches from one of its receiving agents and/or from DFAIT missions. Its agreement with Service Canada includes a requirement that Service Canada "promptly notify Passport Canada of any unauthorized disclosure or use of personal information", while the agreement with Canada Post Corporation (CPC) does not.

B.15 We were informed that some past breaches, which could have affected the protection of personal information, had not been reported to Passport headquarters. In our view, when privacy breaches are not routinely reported and analyzed in a consistent fashion, to determine root causes and to prevent such problems from recurring, this represents an important weakness in the overall protection of personal information.

B.16 We also had concerns about a contract between Canada Post Corporation and Passport Canada, and the way incomplete passport applications were being delivered (in clear plastic bags and open bins) to CPC premises. Passport Canada addressed our concerns during the course of the audit by repatriating the mail back of rejected applications to Passport Canada from CPC.

B.17 We believe that the appointment of a Chief Privacy Officer would help to ensure that a more thorough examination of privacy risk occurs.

Information sharing agreements are out of date; internal controls need to be implemented

B.18 Passport Canada has various service and information sharing agreements with DFAIT, its receiving agents, federal government organizations, and provincial and territorial vital statistics organizations (for birth and death information). The principal federal government partners include Citizenship and Immigration Canada, Correctional Services Canada and the Royal Canadian Mounted Police.

B.19 Many of Passport Canada's information sharing agreements are several years old and do not reflect current best practices in privacy. Several lack key privacy clauses: defining, for instance, what personal information will be shared, the limits to the sharing arrangement, the security controls, and the requirements for monitoring and auditing to ensure that passport information is secure throughout its life cycle.

Conclusion

B.20 As previously mentioned, Passport Canada and DFAIT have already responded to these observations and are taking action to address them in response to the recommendations made during the separate audit of Passport operations.