Office of the
Privacy Commissioner
of Canada

Commissariat à la
protection de la vie privée
du Canada

Privacy Audit of Canadian Passport Operations

December 2008

Table of Contents

Executive Summary

1.1 The objective of this audit was to assess the extent to which Passport Canada (PPTC) is managing personal information in a way that protects the privacy of Canadians. The audit commenced on October 12, 2006. Field work was completed on January 31, 2008, representing the effective date of our observations and recommendations.

1.2 During the course of the audit, we observed that Passport Canada is an organization dedicated to service and the integrity of the Canadian passport. We also note that the organization is under considerable pressure to respond to an unprecedented influx of millions of new passport applications.

1.3 While observing good privacy features, we found weaknesses in a number of areas that require management's attention at PPTC and the Department of Foreign Affairs and International Trade (DFAIT). In the collective, these weaknesses pose an appreciable privacy risk to the overall protection of Canadian's personal information. We conclude that the privacy management framework for passport operations needs strengthening in a number of important and interrelated ways. For this purpose we make fifteen recommendations (see Annex A).

1.4 We wish to thank numerous employees at PPTC and DFAIT for their assistance, cooperation and responsiveness during our audit. Officials acted in a consistently helpful, respectful and professional way.

Collection of Personal Information

1.5 We have concerns about PPTC collecting certain sensitive personal information on a single passport application form. In particular, we are concerned that an applicant's credit card information and guarantor information is collected along with other identifying information (e.g., name, address, phone number and date of birth) on the same application form, as well as the continued acceptance of the SIN card and number as identification. These collection issues may increase the risk of identity theft for Canadians, if this information was inappropriately used or disclosed.

Controlling Access, Use and Disclosure of Personal Information

1.6 Certain controls for limiting access to personal information need attention. They do not always reflect the fact that passport information is defined as "particularly sensitive" "Protected B" personal information according to PPTC's *Information Classification Guide*. We also found that the "need-to-know" principle was not being consistently applied, and that access to information systems was not adequately controlled to ensure that only those employees that need the information to do their jobs have access to it. For example, we found that consular officials at any mission abroad had access to passport files processed by other missions around the world, yet we observed that the need to access this information was infrequent and the information could be alternatively provided as required by DFAIT or by Passport Canada. Wide access to passport files abroad increases the risk of unnecessary exposure of personal information.

1.7 We noted that no one in PPTC or DFAIT is specifically responsible for ensuring that access rights are updated to reflect changes in staff. Although the Information Technology (IT) Help Desk is responsible for changing access rights, they are not always informed of staffing changes or changes in employees' functions affecting access rights. In one case, an employee who had retired six months earlier still had access to a consular system. In other cases, individuals not involved in the passport process had access rights to the consular passport system. Other names were on access lists, although they no longer had access rights.

1.8 More significantly, we found that a basic control on the Integrated Retrieval Information System (IRIS) and Passport Management Process (PMP) systems—an electronic log to track who has looked at completed passport applications—was lacking. In our view, this increases the risk that information on an applicant could be inappropriately used or disclosed.

Ensuring Proper Retention and Disposal of Personal Information

1.9 PPTC archives electronic passport records for up to 100 years. The reasons for doing so are unclear. We noted that this personal information is not encrypted, which increases the risk that it could be inappropriately accessed and misused while in PPTC's custody. Under the *Privacy Act*, information should only be kept while it is useful for administrative purposes or as otherwise prescribed by regulations.

1.10 Certain of PPTC's current practices for disposing of or destroying records containing personal information in hard copy and electronic form are deficient. For example, we found that a number of PPTC and mission locations disposed of passport administrative forms containing personal information in ordinary garbage and recycling bins. At one private-sector shredding facility entire passport photos were visible and documents could be pieced together and made legible even after mechanical shredding.

1.11 We note that using private-sector couriers to transport surplus computer hardware containing sensitive information between PPTC offices entails risk, as witnessed by recent breaches involving this practice elsewhere in the public and private sectors.

Providing Essential Safeguards

1.12 PPTC's and DFAIT ("Consular Services[1]") physical, personnel and IT security systems generally offer adequate privacy protection. However, our audit found certain significant gaps in internal safeguards that should be addressed.

1.13 Based on locations we visited, physical security measures to prevent outsiders from accessing sensitive areas at PPTC and DFAIT locations appeared to be effective for both organizations. However, internal practices for storing passport records and supporting documents (e.g., in clear plastic bags and on open shelves) are inappropriate. In our view, this method of storage of such sensitive records does not adequately protect them from inappropriate or inadvertent access by employees who may not require such access for their job functions.

[1] "Consular Services" in the context of this audit refers to services provided to the public at Canadian missions abroad related to passport and travel documents. Other consular services are provided to the public at these missions, which were not part of our audit examination of Canadian Passport Operations. The organizational area at DFAIT HQ that supports these services abroad is the Consular Services and Emergency Management Branch.

1.14 The design and layout of consular areas in DFAIT missions visited abroad did not provide a consistent level of privacy for clients. Applicants' conversations with consular officials could be overheard by other individuals in public waiting areas at several missions visited. We note, however, that when we called attention to this issue, officials began to address our concerns immediately and indicated that more would be done to improve the situation.

1.15 Difficulties in obtaining criminal and intelligence records in certain countries outside Canada for the purpose of security screening and clearance process for locally engaged "Consular Services" staff (LES)—who may or may not be Canadian citizens—poses a challenge for DFAIT at the same time that PPTC is raising the minimum security screening level for its own employees from "Reliability" to "Secret". However, addressing certain weaknesses noted in our report, such as enhancing access controls over personal information and adding activity tracking features to IT systems could help to mitigate these risks.

Information Technology (IT) Security

1.16 Our concerns in this area relate to the use of portable memory devices and the lack of encryption for certain personal information stored in IT systems and in e-mails transmitted outside DFAIT and PPTC.

1.17 Neither PPTC nor DFAIT has an organizational-wide policy that restricts the use of portable memory devices such as memory sticks, MP3 players and cell phones on PPTC's premises or in the consular areas of DFAIT's missions. Anyone who has access to these locations and to passport information systems could easily photograph, download or copy personal information stored on departmental computers without being detected. Given the inherent risk in using these new technological tools to store sensitive personal information, we believe that it is urgent that both organizations develop and enforce policies covering the use of all portable memory devices on their premises.

1.18 The permanent collection of personal information stored on PPTC's main database, IRIS, and on DFAIT's passport system, PMP, is not encrypted. The lack of this important information management safeguard increases the risk of unauthorized access to this information stored in "clear text", which should be a security concern to both organizations. Please see Annex E (Summary of Passport Information Systems).

1.19 We found that the internal networks of PPTC and DFAIT use encryption to protect e-mails sent to other employees. However, several employees we contacted did not know that e-mails sent outside of the secure internal networks may not be protected by encryption. Any personal information contained in e-mails sent in an unencrypted form to outside networks is vulnerable to interception, copying, modification and improper use by hackers.

1.20 Lastly, we emphasize that our audit was not designed to identify privacy breaches. Indeed, none came to our attention as having occurred during the course of our examination other than the Passport On-line (POL) incident (see paragraph 3.114). Our concern is that given control weaknesses noted above, and without consistent reporting of privacy related incidents, personal information could go astray without DFAIT or PPTC being aware.

Building a Privacy and Security Management Framework

1.21 The overall privacy management of PPTC needs strengthening as evident from our findings above. In this regard, one of our concerns is that PPTC does not have a Chief Privacy Officer (CPO), and that DFAIT has not delegated full Access to Information and Privacy (ATIP) authority to PPTC for privacy matters. Without this authority PPTC must depend on DFAIT's ATIP section to carry out its responsibilities for protecting personal information under the *Privacy Act.* As a result, key privacy responsibilities for the passport program are dispersed and, as discussed later in the observations and recommendations section, have not in our view been given sufficient attention.

An important element in managing privacy and security is to ensure that staff who routinely handle sensitive personal information understand their responsibilities for protecting this information under the *Privacy Act*, and their basic security responsibilities under the Government Security Policy. We found gaps in employees' knowledge in certain areas of privacy and information security. However, we also note that PPTC has begun providing staff with privacy training sessions in these key areas.

Introduction

Why this audit of Canadian passport operations is important

2.1 In fulfilling its mandate, PPTC and its partners collect and use highly sensitive personal information about every Canadian who applies for a passport or other travel document. Some of this information may also be disclosed to third parties for lawful purposes. PPTC currently has more than 30 million passport records under its control.

2.2 Protecting Canadians' sensitive personal information is of critical importance. Should passport information fall into the wrong hands, it could be lost, destroyed, or misused. The theft and misuse of personal information could potentially result in serious consequences to the individual to whom the personal information relates, such as identity theft and financial fraud.

2.3 For these reasons, it is essential that PPTC provide a high level of assurance that it is effectively managing personal information throughout its life cycle—from collection to destruction—no matter where passport applications are processed.

Canada and the global passport system

2.4 Globalization in the late 20th and early 21st century describes the increased mobility of goods, services, labour, technology and capital around the world. Although not a new development, its pace has quickened with the advent of new technologies, especially in the area of telecommunications.

2.5 Globalization has blurred the concept of national borders, allowing trade and commerce to expand, while at the same time facilitating problems such as trans-border human smuggling, organized crime and international terrorism. These risks have resulted in more stringent international demands on travellers seeking passports. Through the United Nations and other international organizations, requirements for the integrity and security of passports have also become more harmonized globally.

2.6 Canada and some 193 other countries worldwide issue millions of passports annually to assist their citizens' safe passage during their international travels. However, passports have evolved from this basic role, and have become an identity document necessary for individuals to participate in the global economy.

2.7 PPTC has stated that "passports have become a primary asset for Canada and Canadians, providing proof of identity and citizenship, evidence in support of entitlement to...government services and benefits, facilitating international travel and commerce, supporting global cooperation in anti-terrorism efforts and contributing to international and domestic security." (Source: PPTC Annual Report 2006-2007, Appendix A, p.1)

2.8 Since the events of September 11, 2001, all countries have been under intense pressure to increase the security and integrity of the passports issued to their citizens. This global imperative has resulted in passport agencies such as PPTC; repatriating passport printing from Canadian missions; introducing new security features to limit passport fraud; increasing the scrutiny of passport applications; and expanding information sharing arrangements with law enforcement and intelligence agencies domestically and internationally.

2.9 Despite fears of terrorism and these increased security controls, Canadians have not stopped travelling. On the contrary, in 2007 alone Canadians made more than 21 million trips outside the country, 16 million of which were to the United States. Most of those travellers had to carry a valid passport or official travel document issued by PPTC or DFAIT to be able to travel abroad.

2.10 The Western Hemisphere Travel Initiative (WHTI) is part of the U.S. *Intelligence Reform and Terrorism Prevention Act* of 2004. On January 23, 2007, WHTI requirements came into force, requiring all air travellers to carry a passport when arriving in the U.S. By June 1, 2009, travellers entering the U.S. by land or sea will also require a passport or other approved travel document, such as the NEXUS card.

2.11 Our audit report has taken into account changes at PPTC and its partners, which have affected the management of personal information that occurred before our audit examination closed on January 31, 2008.

Passport Canada (PPTC)

2.12 Under the *Canadian Passport Order* (SI/81-86) as amended (CPO), the Minister of Foreign Affairs and International Trade (DFAIT) has charged PPTC with the legal authority and mandate to issue, refuse, revoke, withhold, recover, and monitor the use of passports and other travel identity documents for Canadians and Canadian residents.

2.13 PPTC was set up in 1990 as a Special Operating Agency (SOA) within DFAIT to replace the Passport Office. PPTC's SOA status allows it to run its day-to-day operations to some extent like a private sector enterprise, however legally it remains part of DFAIT and is accountable to the Minister of DFAIT. PPTC is also subject to public sector legislation and rules such as the privacy obligations set out in the *Privacy Act*, and in Treasury Board Secretariat (TBS) Guidelines on Privacy and Data Protection.

2.14 The passport application review process at PPTC and DFAIT includes four steps:

- Receipt of completed application along with fees, identity documents, proof of citizenship and other relevant documents at walk-in service locations or by mail;
- Data-entry, document scanning, and the authentication of identity and citizenship;
- Security checks to identify risks, quality control, and passport entitlement decision; and
- Printing and delivery of passports to applicants in person or by mail.

2.15 Based on information available at the time of our audit examination, PPTC employed more than 2,200 people. PPTC's corporate headquarters is in Gatineau, Quebec. Passport processing and service operations are delivered at service locations in the National Capital Region and in four other administrative regions: Eastern/Quebec, Ontario, Central, and Western.

2.16 PPTC has 33 service locations in Canada to serve the public directly and to receive passport applications by mail. Close to 80% of all passport applicants seek walk-in service, while mail accounts for slightly less than 13% of all applications. The remaining applications are dealt with through other service channels such as missions, receiving agents and the Passport On-Line system.

2.17 PPTC and the Consular Services and Emergency Management Branch of DFAIT coordinate the overseas delivery of passport services to Canadians through 139 Canadian missions and over 100 Honorary Consul offices (for Emergency Travel Documents). These missions issued over 136,000 passports as of March 31, 2007, which represents only about 3.5% of Canadian passports issued in the previous fiscal year. While not a significant volume, the delivery of passport services abroad has been described by DFAIT as being "exposed to a high degree of inherent risk."

2.18 Receiving Agents (RAs) – Canada Post Corporation (CPC) and Service Canada (SC) – are under contract with PPTC to receive and screen passport applications at over 150 service locations across Canada. Their role is to collect processing fees and to ensure that applications are complete, before forwarding them on to PPTC for the determination of eligibility. Last year, RAs processed the equivalent of 4.4% of all passport applications. This volume of RA processed passport applications is expected to grow as the number of RAs has increased by over 50% over the same time period.

2.19 As passport applicants financially support the passport program through various service fees, there is a high expectation that PPTC will provide quality and timely service. In its Business Plan 2006-2009, PPTC states that "its primary challenge…is to alleviate service pressures while meeting the need for rigorous security measures." This challenge has been made more difficult as PPTC reports that security responsibilities have resulted in increased costs to issue passports, while the fees charged to Canadians have not kept pace with these costs. PPTC reports it has fallen into a budgetary deficit situation.

2.20 New travel rules in the U.S., along with a strong Canadian economy over the past few years, have resulted in Canadian travellers applying for passports in record numbers. PPTC issued 3.66 million passports in 2006-2007, representing an increase of 22% over the previous fiscal year.

2.21 To face the challenge created by this unprecedented influx of passport applications, PPTC simplified some of its application forms, modified and reorganized its processes, introduced new technology, and moved certain operations.

2.22 Between April 2007 and March 2008, PPTC hired 1,257 employees and 494 left the organization. Furthermore, PPTC grew from 2,091 employees in November 2006 to 3,190 in March 2008. We are informed that this unprecedented increase in staff resulted in a major shift of operational and management resources to assist in the training and coaching of new employees. As a result of this sudden growth and change, there may have been times where required procedures may not have been reflected in the day-to-day work. As the audit was conducted during a period of unprecedented growth in the volume of passport applications, during which time training was being undertaken in a phased approach, some employees observed by the audit team may not have had the full knowledge and experience they possess now that their training has been completed.

2.23 Detailed information about PPTC can be obtained from its website at www.ppt.gc.ca.

Observations and Recommendations

Collection of Personal Information

3.1 Section 4 of the *Privacy Act* describes one of the overriding privacy principles regarding the collection of personal information—that "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the organization." This basic principle ensures that government institutions do not engage in indiscriminate collection of Canadians' personal information.

3.2 The Passport Office has made an organizational commitment "to ensure the information sought from applicants must be justified on reasonable grounds as necessary to the proper administration of the *Canadian Passport Order*."

3.3 We found that the personal information that PPTC collects during the passport process is clearly necessary to fulfil its mandate under the *Canadian Passport Order*, and most of the personal information is collected directly from the individual applicant with his or her consent.

3.4 Passport applicants must provide many pieces of sensitive personal information about themselves, on a single passport form. This personal information ranges from tombstone information such as name, address, phone numbers and date of birth, to employment and residency information, proof of Canadian citizenship, identity card information, travel details, guarantor passport numbers and expiry dates and/or reference information, and applicants' credit card information. Other relevant documents such as a previous passport may also be required by PPTC.

3.5 Other personal information about applicants may also be gathered as necessary from third parties. These parties include Citizenship and Immigration Canada, Correctional Service of Canada, provincial registries, and other law enforcement and intelligence agencies as necessary to determine eligibility and to protect the integrity of the passport system. Passport application forms also include some information about family members, guarantors and/or references.

3.6 In looking at the collection issue we were most concerned about the collection of certain types of personal information on a single passport application document. Sensitive personal information such as financial information, guarantor information and the SIN may be collected, along with many other types of personal information about the applicant as indicated above.

3.7 This "single-form" collection method probably allows for greater efficiencies when processing millions of passport applications. However, by concentrating a broad range of sensitive personal information on one record, it increases the potential consequences for an applicant if anyone were to inappropriately access, use, disclose, destroy or modify the application form.

3.8 **Social Insurance Number (SIN).** Passport applicants must provide information from at least one supporting document listed on the passport application form instructions for identification purposes. This list includes provincial driver's license or health card or other government-issued card. Based on our audit observations, PPTC officials do collect the SIN when an applicant includes it on their passport application form.

3.9 While the SIN is not specifically listed on the passport application form as a document acceptable to support identity, one could interpret the SIN card as being one of the "other federal, provincial/territorial/state or municipal identification card(s)" as described in the passport application instructions.

3.10 We were advised that, while PPTC does not encourage the collection of the SIN as a means of identification, it does accept it if submitted by applicants.

3.11 In addition, the PPTC Policy Manual, DFAIT Passport Training Manual, and the privacy training documents received from PPTC and DFAIT contain no specific instructions to employees to actively discourage applicants from using the SIN as proof of identity for the passport process.

3.12 Our Office has publicly expressed our objection to the routine collection of the SIN for identification purposes, where it is not absolutely necessary or specifically mandated by legislation or by TBS as an acceptable use. The SIN is not just any ordinary kind of identity information. It is considered one of the key data elements sought by identity thieves to carry out financial fraud. Accordingly, collecting the SIN poses a particularly higher level of risk when it is recorded along with other identifying information such as name, address, date of birth and credit card information, all of which are included on a typical passport application.

3.13 The proliferation of the collection and use of the SIN in the public and private sectors has been identified as one of the most important factors that have fuelled the major increase in identity theft and associated fraud related crimes in Canada.

3.14 **Credit Card Information.** Fees are required for each passport application. Passport application forms, when mailed in to PPTC by applicants, include a section that records credit card information including the card holder's name, type of card, number, and expiry date. When this credit card information is provided, PPTC retains this financial information in its electronic information system.

3.15 Because an applicant's credit card information is found with the rest of the information on the application form, both physically and electronically, virtually any employee involved in determining eligibility or issuing a passport could potentially access it. Employees can view this sensitive financial information even if they do not need to do so to carry out their job functions.

3.16 Financial information such as a credit card number is considered to be highly sensitive personal information for Canadians. Once again, financial information when combined with tombstone information and a SIN are the key information ingredients sought by ID thieves and financial fraudsters.

3.17 **Guarantor's information.** We noted another area in which the one-form approach to collecting information could potentially compromise privacy, which relates to the new PPTC guarantor policy introduced in the fall of 2007.

3.18 Under the new guarantor policy, adult general passport applicants may now name almost any adult with a valid passport (including family members and household residents) as guarantor, rather than relying on a narrow list of professionals, as was the case under the old policy. Applicants eligible for the adult simplified renewal passport process are not required to obtain guarantor information.

3.19 Some applicants are still naturally turning to their doctor, lawyer or clergyman to ask them to be guarantors. While no one is under any obligation to act as a guarantor, we are informed that due to their ongoing relationship with certain applicants, these professionals find it difficult to refuse such requests.

3.20 Under the new policy, guarantors must now provide their passport number and expiry data directly to applicants. An applicant enters this information on their application form before submitting it to PPTC in person or by mail.

3.21 A number of these guarantors have complained to our office about having to provide their sensitive personal information directly to an applicant, who could potentially lose or misuse it prior to submitting it to PPTC.

3.22 We recognize that it is important from an operational standpoint for PPTC to collect information as efficiently as possible. However, the need for efficiency must be weighed against the need to ensure the protection of Canadians' personal information.

3.23 Recommendation: PPTC should explore options as to the best method of collection of financial information about applicants and guarantors' personal data that does not unduly impede the passport process, while considering the privacy of these individuals. It should also revise training and policy documents to limit the collection of the SIN, while actively encouraging applicants to use other forms of identification that pose less privacy risk.

Management Response (Passport Canada): Agree. Passport Canada started to re-examine its personal information collection practices to further ensure collection of information crucial to the assessment of client entitlement to a travel document. Passport Canada will review and amend guidelines and training material as it relates to the collection, use and disclosure of personal information practices with particular focus on dissuading clients from submitting SIN as identification. Passport Canada will also create standards and tools for collection practices that will reflect both operational requirements and recommended practices articulated by the Privacy Commissioner. The implementation of these initiatives is planned for 2009-2010.

Controlling Access, Use and Disclosure of Personal Information

3.24 **Access and Use of Personal Information.** As previously mentioned in the report, passport information is "Protected B" information and is described by PPTC as being "particularly sensitive [the compromise of which would create a serious injury to individuals]". Accordingly, we expected to find that PPTC would have consistently applied the "need-to-know principle", and implemented controls to limit employees' access to this information.

3.25 The protection of personal information requires that access to this information be limited to only those employees who have an operational need for it in order to carry out their job functions. Electronic access rights to view, edit, copy or delete this information should also be restricted according to the same need-to-know-principle for IT systems to as few persons as possible without impeding operational requirements. The need-to-know principle and its associated controls work together to limit the threats of inappropriate use or disclosure of this information by an employee, and the subsequent risks to the individual to whom the personal information relates.

3.26 Various administrative, physical and technical safeguards are typically used to control who has access to personal information.

3.27 During our audit, we assessed the extent to which the rights of employees at PPTC and mission "Consular Services" to access passport information reflected their actual roles and responsibilities. While overall we were satisfied that the particular access privileges accorded by PPTC and DFAIT matched employees' roles and responsibilities, we did note some problems.

3.28 In one mission abroad, we found that senior staff had shared their passwords and user identification with junior employees who could gain access to information in the system without the right to do so. In another instance, an employee who had retired more than six months earlier still had access rights to a consular system. Other employees had access rights without being involved in the passport process in any way. Still others were on an access list, although they no longer had access rights. This would appear to indicate that the access list was not being updated regularly at certain missions to reflect changes of staff and employees' roles vis-à-vis the passport process.

3.29 While both organizations must have the capacity to change access rights quickly to respond to sudden or unexpected operational requirements, employees should not be kept on access lists "just in case" an emergency happens.

3.30 We also noted that no central unit at DFAIT or PPTC, such as the IT Service desk is completely accountable and responsible for ensuring that the right to access to information in IT systems reflects current staff and their job functions. The system and process to update access rights relies heavily on individual managers and supervisors advising the help desk of their employees changing job functions or leaving the organization for temporary or permanent periods. IT's monitoring of the accuracy of such lists is limited to spot checks and Human Resources sections at both organizations do not play an active role in informing IT of changes of personnel, which may have been missed by managers or supervisors. The end result is that the current decentralized control system is not always effective in ensuring that such important IT access rights are kept up to date.

3.31 While access rights should be based on an individual's role and functions, access to specific information should be based on a demonstrated operational need. In our review of missions abroad, we found that consular staff had access to far more passport information than they actually needed on a day-to-day basis to do their jobs. Consular access to DFAIT's PMP system not only includes all completed applications from the mission where the employee works, but also all completed records from all other missions abroad. In other words, any mission can look at passport information collected at any other mission. For instance, mission staff in Paris may access completed passport records generated in Beijing, Los Angeles, Mexico City or Moscow, and vice-versa.

3.32 We observed that the need to access this information was infrequent in consular sections and the information could be provided as required by DFAIT or PPTC.

3.33 We also noted that an electronic audit trail log exists for passport applications while processed (i.e. Work in Process (WIP)) by PPTC and for any modifications to completed applications. However, once WIP files are transferred to the IRIS Central Index (CI) files permanent collection, the WIP audit trails are deleted. We found that the IRIS-CI and PMP permanent collections do not have audit trail capability to record when an individual has viewed a completed passport file.

3.34 Audit trails are basic control features on IT information systems to ensure that authorized users do not abuse their access privileges by accessing personal information for non-job-related reasons. We were surprised that such a safeguard did not exist to track who had viewed completed passport files on either DFAIT's PMP or PPTC's IRIS – CI systems.

3.35 Later in the "Safeguards" section of the report, we will elaborate on the security risks that exist because PMP and IRIS electronic passport information is not stored in an encrypted format. When considered with the access rights and audit trail issues just mentioned, the cumulative effect of such information security gaps, when considered together, may result in an even more serious risk for Canadians' passport information.

3.36 ***Recommendation: PPTC and DFAIT should jointly take steps necessary to control employees' access to personal information. These steps should reflect its Protected-B classification, follow the need-to-know principle, and include electronic audit trails for IRIS and PMP systems to minimize the risk of inappropriate access to personal information.***

Management Response (DFAIT): Agree. DFAIT has implemented audit trails in May 2008 for logging when an individual has viewed certain elements of a consular service request. These capabilities will be further improved in the near future.

DFAIT and Passport Canada will also work collaboratively to ensure that both IRIS and PMP have necessary program and technical safeguards to minimize the risk of inappropriate access to personal information.

Management Response (Passport Canada): Agree. In 2007-08 Passport Canada has completed review and re-alignment of all IRIS user profiles to more accurately reflect the need to know. In addition, the new data entry tool that will be implemented during this fiscal year will have enhanced logging capability over IRIS and will be linked to the IRIS profile system. Passport Canada and DFAIT will work collaboratively to ensure that both IRIS and PMP have necessary program and technical safeguards to minimize the risk of inappropriate access to personal information.

3.37 **Outsourcing the "Mail-Back" Function to Canada Post Corporation (CPC).** Under the terms of a contract between CPC and PPTC, Canada Post was made responsible for picking up incomplete passport applications and supporting documents from PPTC headquarters and transporting this information to a CPC facility in Ottawa. CPC would then verify the contents of each file and mail the information back to applicants.

3.38 We had concerns about the way the documents were being delivered (in clear plastic bags and open bins) to the CPC facility under the contract. We were also concerned about the fact that CPC employees had access to complete application forms and supporting documents, including the sensitive personal information they contained.

3.39 We wrote to PPTC on June 28, 2007 about this outsourcing arrangement. PPTC provided an initial response on September 5, 2007, to which we responded with additional concerns on February 18, 2008. On March 14, 2008, PPTC advised the OPC

that effective April 1, 2008 all activities related to the mailing back of rejected passport applications would be repatriated to PPTC from CPC.

Ensuring Proper Retention and Disposal of Personal Information

3.40 The *Privacy Act* takes a life-cycle approach to the protection of personal information; which is collected and disclosed for administrative purposes and must subsequently be securely disposed of when it no longer serves such a purpose.

3.41 Under the *Library and Archives of Canada Act*, government institutions are required to develop retention and disposal schedules that define how long corporate information (including personal information) can be kept before it is destroyed or archived.

3.42 Our audit examined the procedures for retaining and disposing of paper based and electronic records containing personal information at PPTC and RA locations in Canada and at DFAIT consular sections at missions abroad.

3.43 **Retention.** In the case of PPTC, paper passport applications and records are generally retained for approximately six weeks after they have been processed, and then they are destroyed. Original documents submitted as proof of Canadian citizenship are returned to applicants. Expired and cancelled passports, which are not returned to applicants, are physically voided and destroyed soon after the new passport is issued.

3.44 In the case of DFAIT, completed passport applications not required by PPTC are retained for 90 days after the end of the month during which the application was processed. The applications and all related documents and photographs should then be shredded using approved cross-cut shredders.

3.45 However, the electronic version and microfilm copies (made prior to 2002) of passport information at PPTC and electronic records at DFAIT may be retained for up to 100 years.

3.46 PPTC retains electronic passport information in two large data banks, one in the Greater Toronto Area and the other in the National Capital Region, which together contain a critical mass of over 30 million passport applications filed by Canadians. As previously mentioned, this is particularly sensitive information.

3.47 The vast quantities of passport information collected every year from millions of Canadians is the principal informational asset that PPTC requires both to ensure the integrity of the passport process and to deliver passports to Canadians in a timely fashion.

3.48 But for as long as this particularly sensitive passport information is retained by PPTC, it also represents a liability. This liability flows from the risk that sensitive information may potentially be inappropriately accessed or misused while it is in the custody of PPTC.

3.49 From our discussions with officials at PPTC, it is not clear why passport information is being retained for as long as 100 years. This retention period appears to be longer than necessary to serve PPTC administrative and program needs and creates an unnecessary risk for Canadian's passport information simply by having it there.

3.50 ***Recommendation: Given the risks inherent in retaining passport information for a 100-year period, and considering the requirements of the Privacy Act to retain personal information only for as long as necessary or as defined in regulations,***

PPTC should consult with Library and Archives Canada to reassess this exceptionally long records-retention period.

Management Response (Passport Canada): Agree. The retention period for passport information was revised to 100 years in December 2006: an active period of 12 years followed by a dormant period of 88 years before being transferred to Library and Archives Canada. The dormant period of 88 years allows for retention of client's passport history which is crucial to identity verification and ongoing entitlement to a passport. Passport Canada will revisit this retention period over the next three years as new programs and technologies such as the simplified passport renewal process and facial recognition may influence the retention and disposition period of passport applications.

3.51 **Disposal.** We noted weaknesses associated with the transportation and destruction of personal data held on paper records and computer devices (e.g., computer hard drives and other data storage media). The transportation of passport information between PPTC and CPC mentioned above is an example of the kind of risks involving sensitive personal information being sent from one physical location to another.

3.52 In a number of PPTC and mission locations, certain passport processing forms containing personal information, such as names and dates of birth of individual applicants, were found in regular garbage and recycling bins without having been shredded. At one Service Canada (SC)[2] location, the destruction of passport information had been outsourced to a private contractor. When we visited the contractor's premises, we found that SC did not systemically supervise the transportation and destruction of sensitive passport records.

3.53 We also noted that, even after the documents had been apparently shredded, entire passport photos remained intact and other application information could be easily pieced together and made legible, exposing this information to potential inappropriate access or use.

3.54 As there is always a higher element of risk when transporting records off-site for destruction, on-site disposal should be the method of choice when possible. By eliminating the off-site transportation of personal records and by ensuring the physical destruction is carried out on secure premises by government employees, a government department can have a greater level of assurance that the personal information of Canadians is being adequately protected.

3.55 This is not to say that records can not be destroyed off-site or by a contractor, but these options require stringent controls (e.g. monitoring, record keeping and quality control) to mitigate the higher risks inherent with such arrangements.

3.56 In addition to the hard-copy passport applications it stores, PPTC also maintains a large amount of computer data at its facilities. A major hard drive or back-up computer tape may potentially contain passport records on millions of Canadians.

[2] Service Canada and Canada Post Corporation have signed contracts with Passport Canada to provide limited passport services to the public at many of their existing service locations across Canada.

3.57 When computers and the information they contain have reached the end of their useful life cycle, a secure method of disposing of this information is required, based on an assessment of privacy and security threats and risks.

3.58 PPTC has an IT security policy that clearly defines how electronic information storage devices are to be disposed of and destroyed. This policy stipulates that backup tapes and hard drives are to be delivered to IT staff at PPTC headquarters, where government approved procedures are used for destroying the data by making it illegible and irretrievable. According to this policy, the Information Protection Centre will make arrangements with the client for the pickup or drop-off of the media if located at headquarters. All items transmitted to headquarters from regional offices are to be sent by secure mail.

3.59 At the time of the audit, we found that the PPTC regional offices were transporting redundant computer devices to headquarters via commercial courier services for disposal and destruction. In reviewing literature, we have noted that several serious privacy breaches have occurred elsewhere in recent years in the public and private sectors, when couriers were used to transport hard drives and other information storage devices containing sensitive personal information between offices.

3.60 ***Recommendation: PPTC should assess the privacy and security risks relating to its current practices for disposing and/or destroying sensitive personal information for all types of records.***

Management Response (Passport Canada): Agree. Passport Canada's Corporate Records division disposes and destroys sensitive information contained in all types of records in conformity with the Government Security Policy. Furthermore, Passport Canada implemented procedures for sanitization and destruction of sensitive media. Passport Canada will work with DFAIT and Service Canada to determine appropriate collection, retention and disposal of passport related information.

Providing Essential Safeguards

3.61 The important preamble to the *Privacy Act* states that its purpose is to "extend the present laws of Canada that protect the privacy of individuals". Sections 4 to 8 of the *Privacy Act* also stipulate that personal information may only be collected, used or disclosed for an administrative purpose or as otherwise prescribed. Therefore the security and safeguarding of personal information is important to meeting the protection expectation set out in the *Privacy Act*.

3.62 The Government Security Policy and other related directives define what kind of safeguards are appropriate for information based on its sensitivity and the impact of its compromise on the government and/or its citizens.

3.63 PPTC and DFAIT ("Consular Services") have instituted a layered and holistic approach to information security that is designed to protect Canadians' sensitive passport records and limit known threats and risks to these records. This approach includes physical, administrative, personnel and IT security elements, which, taken together, generally offer adequate privacy protection. Despite these existing safeguards, our audit found some significant gaps in the internal controls that could expose personal information to loss,

misuse or inappropriate disclosure. Some of these gaps have been mentioned above as they related to earlier issues and still others are elaborated upon below.

3.64 **Physical Security.** Physical security measures include—but are not limited to—locked doors and cabinets, intrusion alarm systems, security guards, and controlled access to sensitive areas in facilities. Physical safeguards help to protect personal information by preventing the public, and employees who do not require access to this information, from entering the operational areas where the personal information is collected and processed.

3.65 The PPTC and DFAIT locations visited appeared to have good physical safeguards to prevent outside intruders from accessing passport information. Although such perimeter protection is important, it is still necessary to store sensitive personal information properly and limit access to it within an organization's premises.

3.66 As previously mentioned, passport information is particularly sensitive personal information. Because of the sensitivity and concentration of personal passport information at DFAIT mission and PPTC locations, this information should be considered at the high end of the Protected B scale and may warrant additional protection beyond that prescribed for less sensitive Protected B information.

3.67 One common internal physical security issue that we noted at virtually every PPTC office and DFAIT mission visited was the way passport records and supporting documentation were stored. As previously mentioned, passport applications and supporting documents are placed in clear "Zip-lock" like plastic bags. These sensitive records remain in these bags from the point at which they are received by PPTC, missions and RAs, until the time the printed passports are issued to applicants. For DFAIT, this audit observation applies to all five missions visited in Beijing, Berne, Los Angeles, Paris and Taipei.

3.68 We have two concerns with this practice. First, any employee with physical access to the facilities could view sensitive personal information visible through the clear plastic bags. Second, the storage of passport documents—including original supporting documents as well as expired and new passports—on open shelves or in open bins does not adequately protect these documents from being inappropriately accessed, used, removed, disclosed, or destroyed by any employee who has physical access to them.

3.69 In addition, we were informed that if a bundle of completed passport application forms were to be removed from PPTC or mission premises, officials would have no way of knowing that these sensitive documents have gone missing as they are not tracked after passports are issued. While these records no longer serve an administrative purpose after a passport is issued, they do not cease to require privacy protection because of the sensitive personal information they contain.

3.70 At several PPTC and mission locations we also observed faxes and e-mails containing personal information being stored in open containers overnight.

3.71 It is important to note that some consular areas and PPTC locations did lock up passport records in cabinets at night, while the majority of locations visited did not. Even those locations with cabinets to lock up records did not systematically do so.

3.72 The audit team also noted that at certain consular sections abroad, employees who did not work in these sections could nevertheless access them, and that these employees would sometimes accompany a member of the public seeking passport services. We were assured that consular staff would always be present whenever these visitors were within the consular area. However, these individuals could potentially see or access

sensitive passport information, including expired and new passports, original identifying documents and application forms kept in clear bags, in open bins and on open shelves. During our audit examination, no reasons were provided why these applicants could not be served at the public service counter outside the operational consular processing area.

3.73 A similar situation involving persons having inappropriate physical access to passport facilities was noted at certain PPTC locations. Some security guards were allowed regular access to PPTC processing areas where personal information was exposed on desks and open shelves, although their role should not require them to do so unless there was a security incident. Also some cleaning staff, apparently lacking security clearances, were permitted unescorted access to PPTC facilities.

3.74 Another important aspect of internal physical security measures relates to the design and layout of facilities where clients are served. We found that the layouts at some PPTC and RA locations did not provide adequate distance between clients for the privacy of conversations at the service counter. In these locations, conversations could easily be overheard by others. It was also possible at a number of service locations visited for one client to look over the shoulder of another or to look sideways and view the personal information of another client.

3.75 With respect to the layout of many consular client service areas at DFAIT missions visited, we found inconsistency in terms of the adequacy of the physical privacy provided to their clients. Some public waiting areas were excellent and others were poor in their layout. For example, the public waiting area at the Taipei Trade mission was well-designed from a privacy standpoint and could be a model for other locations.

3.76 Public service areas in missions such as Beijing and Paris posed several privacy problems for clients. We noted that DFAIT had installed separate enclosed areas at these locations intended to ensure the privacy and confidentiality of consular discussions with clients, however the design of these rooms appeared, on the contrary, to amplify the volume of clients' private conversations with consular staff. In addition, the set up for clients waiting in chairs or in a queue often did not leave an adequate distance between the service counter and the other clients waiting their turn to be served.

3.77 While certain of these situations can not be readily corrected because of the physical layout of certain mission locations, in other cases, minor modifications can be made to enhance the privacy of clients.

3.78 It is important to note that mission officials at several locations visited took immediate corrective actions to improve the privacy of their clients, when informed of our observations at the time of our audit examination visit. We were also informed that other steps will be taken to further increase the privacy of applicants in public waiting areas.

3.79 ***Recommendation: PPTC and DFAIT should ensure that paper-based files containing passport information are stored in a manner appropriate for particularly sensitive "Protected-B" information according to the Government Security Policy.***

Management Response (DFAIT): Agree. DFAIT provides the proper security containers for the storage of Protected B information, in accordance with the Government Security Policy. This practice is reviewed during routine security inspections. Where containers are viewed as deficit arrangements are made to provide appropriate equipment. In addition, procedures for storage of materials are reviewed with the appropriate manager.

Management Response (Passport Canada): Agree. Physical security measures such as electronic access and controls, access authorization levels, security zoning in the design and fit-up of Passport Canada offices and the existence of systems (CCVE systems) located at strategic points throughout each office, reduce the risk of loss, theft, destruction, and compromise to the personal information. Passport Canada will continue to ensure that paper-based files containing passport information are adequately protected against identified threats and risks through ongoing physical security reviews and compliance audits and protection of personal information and security awareness training. Passport information files which must be retained in a paper-based format are stored in protected-B security area with restricted access according to the Government Security Policy.

3.80 ***Recommendation: PPTC and DFAIT should review physical and other safeguards to ensure that only persons who have an operational need to enter areas where passports are processed are allowed to do so.***

Management Response (DFAIT): Agree. At missions overseas, DFAIT ensures that access to the areas where passports are being processed is controlled through a variety of measures: the person must have the appropriate security screening and they are provided with key pad access codes to enter the area. Managers and appropriate staff are briefed on the protocols and measures that must be followed. This is reviewed during mission inspections.

Management Response (Passport Canada): Agree. Passport Canada's Physical Security Section risk reviews and evaluations are scheduled for selected offices on a yearly basis to ensure that appropriate measures are in place to protect assets based on the identified threats and risks. Physical security measures such as electronic access and controls, access authorization levels, security zoning in the design and fit-up of Passport Canada offices and the existence of systems (CCVE systems) located at strategic points throughout each office, increase security to ensure that only persons who have an operational need to enter areas where passports are processed. Passport Canada will continue to monitor and evaluate the adherence to and effectiveness of its physical safeguards.

3.81 ***Recommendation: PPTC and DFAIT should review the layout and acoustics of all public service locations to ensure that they provide an adequate level of privacy for their clients through appropriate sight and sound barriers and signage.***

Management Response (DFAIT): Agree. During security inspections DFAIT reviews the layout and acoustics of public service locations. Where possible, re-configuration of the area is undertaken. This is an on-going process, with the most sensitive locations being addressed first.

Management Response (Passport Canada): Agree. Current Passport Canada fit-up standards approved by PWGSC include features that ensure the present standard of privacy required of all public service agencies offering counter service to the public. As Passport Canada offices are relocated or renovated, representing a maximum 10 year time frame, additional and improved privacy features are being incorporated in the design concepts of our office layouts.

3.82 **Personnel Security Screening.** While a security clearance does not guarantee the reliability of an employee on its own, it is a useful and objective screening tool for ensuring that individuals with a criminal record or of doubtful reliability are not hired to a position of trust that involves handling Canadians' sensitive personal information.

3.83 The basic personnel security level for employees handling "Protected" information is called "Reliability" and involves a criminal record and other basic checks.

3.84 According to the Treasury Board Personnel Security Standard, "Personnel screening must be carried out according to the highest level of information and assets." A PPTC Report on passport services at Canadian missions abroad indicates that "Passport inventory is a national security asset and is afforded Secret Classification". In addition the Information Classification Guide provided by PPTC during the course of the audit defines "material serving in the production of passports (e.g. Blank passports) "as Classified information at the Secret level." These provisions would normally mean that individuals handling passport blanks should therefore have a Secret Clearance.

3.85 DFAIT informs us that "at missions abroad, it has implemented procedures that limit access of Protected B information to those who have been granted Reliability Status, have a 'need to know' and have the approval of the Program Manager (e.g., CBS consular officer) and the Mission Security Officer. Locally engaged staff do have access to emergency and temporary passport blanks and prepare these passports as required under the close supervision and review of a Canada based security cleared officer following very specific procedures. These procedures are reviewed during mission security audits." We did not verify this representation.

3.86 Both the Secret and Top Secret security screening processes entail collecting more extensive information from the employee as well as a more intensive review of this information by the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) than does the basic "Reliability" check. We were informed however, that CSIS is also involved in the security screening process for Locally Engaged Staff (LES) at missions, although the type of screening checks performed by CSIS for DFAIT were not defined.

3.87 In anticipation of new, more stringent TBS personnel security guidelines, PPTC has been raising the level of personnel security screening it requires for its operational employees from the basic Reliability level, to the higher Secret level. However, many consular employees, including most LES and the employees of receiving agents still have "Reliability".

3.88 We acknowledge that in many countries around the world, criminal and intelligence records are not as readily available as they are in Canada and certain western nations. This situation would make it more difficult for DFAIT to obtain Secret security clearances for its LES staff in these countries. We do not call into question the integrity or loyalty of LES staff, but only point out the limitations of verifying personnel security overseas according to domestic standards. The LES staff we selected for interview appeared knowledgeable and committed to their work in processing passport applications. However, in our view, DFAIT is assuming a higher risk for LES that are not cleared to the Secret level.

3.89 In a 2006 report of passport services at Canadian missions abroad, PPTC indicated that "there are 167 Canadian Based Staff (CBS) and 284 Locally Engaged Staff (LES) contributing to the passport program abroad". All CBSs are Canadian citizens employed by DFAIT as Foreign Service Officers (FSO), while the majority of LESs are not Canadian citizens.

3.90 The supervision of "Consular Services" and its passport program is always carried out by a CBS officer at each mission. However, Canadian based Foreign Service Officer (FSO) positions tend to rotate from mission to mission and from role to role frequently, while — LES as they live in the country where the mission is located — tend to work for longer periods at that particular location and in the same function. Therefore, new consular FSO officials rely heavily on the experience and trustworthiness of LES for passport processing matters. Several LES, even at an intermediate level, are responsible for determining passport eligibility without direct review by a CBS.

3.91 While it is not our role to tell DFAIT who should determine the eligibility of passport applicants, this particular situation at "Consular Services" abroad, as well as our discussion about the security clearance process for LES, does raise an issue about the adequacy of such supervisory arrangements for the protection of Canadians' personal information.

3.92 In our view, given the combination of factors when issuing passports abroad, including: the dispersal of passport functions at 138 missions and over 100 Honorary Counsel offices (for emergency travel documents); the lack of certain IT controls at missions; the differing security levels between LES and CBS employees; and consular service employees' broad access to passport information; there is a greater risk that a privacy breach may occur.

3.93 Given the importance of LESs contribution to the passport program overseas, it would be unreasonable to expect DFAIT to stop availing themselves of their services. Nevertheless, there may be some steps that DFAIT should consider to mitigate the inherent risk associated with using LES's in the delivery of the passport program abroad.

3.94 ***Recommendation: PPTC and DFAIT should ensure that all employees and contractors handling passport information have adequate personnel security clearances, as required by the Government Security Policy and Treasury Board Policy. Any contractors, cleaning staff or visitors lacking security clearances should be escorted at all times by a PPTC or DFAIT employee.***

Management Response (DFAIT): Agree. Canada based staff posted abroad require a Top Secret clearance. In exceptional cases, for urgent operational reasons, they may proceed to post with a minimum Secret, with Top Secret in process.

Locally Engaged Staff are granted a Reliability Status which is the minimum security screening level prescribed by the Government Security Policy. Locally Engaged Staff are granted access to Protected B information only on the approval of the Program Manager and the Mission Security Officer. DFAIT enforces the requirement of the Government Security Policy for contractors, cleaning staff or visitors. Visitors and contractors are provided mission access under escort. Cleaning staff are under escort in all areas where sensitive material is processed.

Management Response (Passport Canada): Agree. Passport Canada ensures that all employees, contractors, cleaning staff and any other individuals having access to PPTC premises in Canada or sensitive information are appropriately screened according to the requirements of the GSP before commencing work. Visitors are not issued access cards and instead are escorted at all times by a designated Passport Canada employee. Passport Canada will continue to ensure that existing screening policies are consistently adhered to.

3.95 ***Recommendation: Where it is impossible to obtain equivalent personnel security clearances for Locally Engaged Staff at missions, DFAIT should place increased reliance on access controls and audit trails.***

Management Response (DFAIT): Agree. As noted in Recommendation 3.94 above, Locally Engaged Staff are granted Reliability Status which is the minimum security level prescribed under the Government Security Policy. Locally Engaged Staff have been through a screening process. In addition, it is difficult for DFAIT to conduct security clearances abroad.

3.96 **IT Security.** Earlier sections of this report discussed access to information stored in IT systems. One section noted weaknesses relating to the inappropriate use of passwords. The other indicated a need to institute an electronic audit trail for tracking the access and use of personal information stored in IT systems. Please see Annex E for further details about passport IT systems.

3.97 Our audit also raised two other IT security concerns relating to the use of portable devices and the lack of encryption for certain systems and information.

3.98 **Use of Portable Information Storage Devices.** Over the past decade, the use, variety and information storage capacity of portable computing and electronic “memory” devices have increased exponentially. Cell phones now take digital pictures. Pocket-sized memory sticks may store more data than some desktop computers could only a few years ago. BlackBerries can transmit large data files wirelessly around the world. These

electronic storage devices have become indispensible in the private and public sectors. Employees often carry their own devices as well as those issued by their employer.

3.99 As employees and employers increasingly introduce these devices into workplaces, they also introduce new risks for the protection of personal information. These new technologies can easily and quickly be used to photograph, copy, record, download, transmit, or remove large quantities of information with little risk of detection. It is also important to note that such devices can also introduce computer viruses from outside systems.

3.100 In addition, all electronic devices, particularly wireless devices, can be easily adapted to act as a microphone, recorder or clandestine transmitter, even when turned off. Hand-held devices, because of their size, are easily lost, misplaced or stolen.

3.101 In a document regarding the use of wireless devices at missions, DFAIT states that "the presence of wireless devices where privileged government business is taking place, whether verbal or electronic, can be a danger to the confidentiality of information."

3.102 During our audit examination at passport locations and missions abroad, we noted that passport employees and consular staff routinely carry cell phones or BlackBerries. Restrictions do exist in certain areas of Canadian missions, which are not part of "Consular Services", about the carrying and use of such devices. In these areas cell phones and personal digital assistants must be left at the door before entering the restricted area. Similarly, PPTC has issued a directive banning cell phones or handheld devices within PPTC's print centres, but this directive does not apply to other passport processing areas.

3.103 We also found that neither PPTC nor DFAIT have a policy that restricts the use of portable memory devices such as memory sticks, MP3 players and cell phones in all PPTC premises or in the consular areas of missions.

3.104 At the time of our audit, neither PPTC nor DFAIT had a way to track or prevent the use of devices such as USB memory devices on their passport systems. Also we noted that there is no program of periodic and random security checks to ask staff leaving a mission after a day's work whether they have in their possession any office documentation in paper or electronic form containing personal information associated with the processing of passport applications. In our view, controls should augment and support the reliance placed on the integrity of everyone working in missions abroad, and indeed those working in passport operations in Canada, given the highly sensitive nature of passport information.

3.105 Considering that this issue could be one of government wide import, we discussed it with Treasury Board Secretariat officials. We asked these officials whether they thought there was enough guidance issued to date to deal with risks posed by such emerging technologies. TBS informed us that while a singular comprehensive document is not available, the various guidance documents issued to government departments are sufficient. They added that each department is responsible for assessing the risks inherent within their own organization related to the use of portable devices, just as they would for any IT system, under the Government Security Policy and related policies. Departments should normally conduct a threat and risk assessment and ensure that appropriate policies, practices and other controls are in place to deal with risks specific to their own operations – which can vary from one program to another and from one department to another.

3.106 It is important to note that the scope of our audit did not include an assessment of TBS guidance. We note, however, that at least one province (Ontario) has issued comprehensive guidance about the use of portable devices. What we have observed regarding PPTC and DFAIT "Consular Services" might serve as a reminder to other federal departments and agencies to assess their existing policies and procedures controlling the use of portable devices.

3.107 **Encryption of Passport Information.** The encryption of sensitive personal information stored in databases or transmitted by e-mail provides an important security safeguard for preventing the unauthorized interception or use of this information. Encryption is a means of protecting information by scrambling its contents so that it can not be understood by unauthorized individuals. Only persons with authorization and decryption keys can decipher encrypted information and make it readable again.

3.108 We found that the passport information stored in PPTC's main database IRIS and DFAIT's PMP system is not encrypted. PPTC has indicated however that it has been studying the possibility of adding an encryption feature to its future update or replacement of the IRIS system.

3.109 PPTC and DFAIT use secure internal networks to protect e-mail transmissions sent to other employees. Similarly, e-mails sent to other departments with compatible security protocols are also secure.

3.110 However, for the many e-mails destined for recipients outside these closed networks, the personal information they contain is vulnerable to interception, copying, modification or destruction by a hacker. Through discussions with various DFAIT employees abroad and at headquarters, it was apparent that some employees incorrectly thought that all external e-mails, even those outside the DFAIT secure network, were protected.

3.111 Under the Government Security Policy, each department is responsible for assessing risks related to the storage and transmission of its records. Treasury Board has issued guidance about the use of encryption tools for Protected B information and the Communication Security Establishment can assist departments in their choice of encryption methods.

3.112 ***Recommendation: PPTC and DFAIT should develop a policy limiting the use of portable memory and recording devices on their premises, and explore the feasibility of controlling the ability of staff to connect these devices to internal information systems. Employees should be informed of this policy and notices should be posted at main entrances to passport processing areas. In addition, periodic sweeps should be carried out to ensure that this policy is respected.***

Management Response (DFAIT): Agree. DFAIT conducts ongoing reviews of policies including use of portable memory and recording devices. In addition, emphasis is being placed on enhanced security education, awareness and training. Physical security and IT security inspections currently review existing information technology and physical security policies and procedures.

Management Response (Passport Canada): Agree. Passport Canada will review current policy gaps in respect to the use and general management of all portable devices (memory cards, Blackberries, etc.) as well as the access to our systems using such devices, and will subsequently develop policies and procedures as required.

3.113 ***Recommendation: PPTC and DFAIT should consider encrypting all passport information stored on the IRIS and PMP systems to better protect it from inappropriate access, and develop strategies for ensuring that all e-mails containing personal information that are sent outside of secure networks are encrypted or otherwise sent by a secure means.***

Management Response (DFAIT): Agree. Work is ongoing at strengthening information protection practices and the Department is actively working at improving information technology security, security awareness, and education. Further, we will enable encryption of the network link between Passport Canada and DFAIT which is used to exchange data between PMP and IRIS. DFAIT will consider encrypting passport information stored in databases used for the PMP system.

Management Response (Passport Canada): Agree. Passport Canada is in the process of replacing the Central Index system as well as implementing new security case management (SICMS) and facial recognition systems. In the context of those projects, Passport Canada will study and adapt the most appropriate options for strengthening safeguards for the protection of personal information stored in our electronic systems. Passport Canada will also launch a secure network project to assess other security aspects with the goal of developing a comprehensive departmental strategy to strengthen our information protection practices. In order to address some of the immediate concerns, we will enable encryption of the network link between Passport Canada and DFAIT which is used to exchange data between PMP and IRIS.

3.114 **The Passport On-line (POL) System.** Since February 2005, PPTC has permitted Canadians to fill out their passport applications over the internet using the POL system. We were informed that, on average, the POL stores about 28,000 active on-line passport applications at any one time.

3.115 Applicants access POL through “epass”, the federal government’s secure interface for all Government On-Line programs and services. Each POL application has an active period of 60 days. After filling out the application on-line, the applicant is asked to print a copy and bring it in to his or her local passport office.

3.116 In December 2007, the OPC learned through the media of a breach of the POL system. An individual had informed PPTC that while on the POL system, he had discovered that he could access other applicants’ sensitive passport information. This information included their driver’s license number, SIN or health card number, as well as their address and phone number. He was able to do this by merely randomly changing one number in the Uniform Resource Locator (URL). A URL is the unique alpha-numeric locator that appears at the top of each webpage on every internet site.

3.117 Soon after becoming aware of the breach, PPTC shut down the POL system and corrected the programming problem, effectively preventing any other inappropriate access to personal information. At the time of our inquiries in December 2007, PPTC advised us that they were only aware of this one breach of this type, which involved one person accessing a small number of records about other applicants. Given that it was

the same individual who brought the breach to the attention of PPTC, the risk to Canadians' passport information was considered by PPTC to be minimal.

3.118 Part of our audit of PPTC's IT systems involved reviewing their System Development Life Cycle (SDLC) IT control framework. The SDLC is the complex process by which all computer programs are reviewed and validated before they are put into production or are modified. This multi-step internal review and approval process is intended to ensure that such programs are operating properly, and that they are capable of protecting information from inappropriate access. Our review found that PPTC had a reasonably strong SDLC process, with the necessary resources and practices, and this process has been reviewed by the Communications Security Establishment.

3.119 The gap in the system, which was brought to light by the breach, was likely caused by human error, which can be limited, but not totally eliminated in any complex IT system. However, PPTC is investigating possible solutions to prevent a similar breach from recurring in the future.

3.120 When we completed our audit examination on January 31, 2008, PPTC was conducting its root cause analysis in an attempt to pinpoint the origin of the problem and the extent to which others may have inappropriately accessed someone else's passport information through the POL system. Potentially, a coding flaw could have been present since the POL system was first established. Once PPTC has completed its investigations, we will be following up to review the conclusions. PPTC has committed to providing OPC with a copy of its investigation report.

3.121 The audit team was also informed that PPTC will be implementing a replacement for the current POL system over the next year using a method to encrypt and protect personal data.

Building a Privacy and Security Management Framework

3.122 Given the volume and sensitivity of personal information that PPTC manages, the complex service-delivery model involving domestic and overseas partners, and the expectations of Canadians relating to their privacy; PPTC is expected to fulfil its privacy responsibilities according to the *Privacy Act* and TBS guidelines and provide the highest level of privacy protection possible. PPTC has developed a number of elements of a framework for managing privacy and ensuring that the personal information in its custody is secure. However, we found that certain key components of the framework were missing or deficient.

3.123 **Accountability for Privacy.** A 2006 Audit Report by DFAIT of passport services at missions indicated that "the inherent risks of the highly distributed nature of roles and responsibilities, combined with the newness of the Foreign Operations Division [at PPTC], could be reduced by clearly defining governance structures, lines of accountabilities, delegations of authority, and by defining and communicating a clear, formal path of escalation for passport-related issues originating abroad."

3.124 The creation of the Foreign Operations Division within PPTC's Security Bureau to coordinate consular passport services with DFAIT is a positive example of PPTC's efforts to reinforce accountability and control of consular passport operations. While progress such as this has been made since the DFAIT report was issued, other aspects of the

management control framework between PPTC and DFAIT are still missing or are inadequate in the areas of the protection of personal information.

3.125 As personal information about Canadians is the raw material essential to PPTC's operations and carrying out its mandate, we expected that the protection of this sensitive information would be a strategic priority at PPTC. However, at the time of our audit, the protection of personal information was not articulated as one of PPTC's core mission objectives. The PPTC corporate objectives focus on: first, ensuring the integrity and security of the eligibility process and second, maintaining high service standards to the public. While we do not question the validity of the core objectives chosen by PPTC, we consider the objective of pursuing excellence in the protection of Canadians' passport information would complement and reinforce the other two.

3.126 We also noted that PPTC does not have a Chief Privacy Officer (CPO) or other senior official who is accountable for all privacy responsibilities related to the protection of personal information.

3.127 While it is not a legislated requirement under the *Privacy Act* for government institutions to name a senior official as CPO, more and more departments and agencies managing significant personal information holdings are naming a CPO in recognition of the growing importance of privacy issues for Canadians and how privacy breaches can impact on an organization's credibility with the public and its national and international partners.

3.128 The appointment of a CPO also helps to ensure that privacy issues have a champion at the corporate decision-making table, while ensuring the accountability for the coordination and consistent implementation of the many elements of a privacy program across an organization.

3.129 We also found that DFAIT has not delegated full Access to Information and Privacy (ATIP) authority to PPTC for access to information and privacy matters, although an ATIP Coordinator and additional staff were hired by PPTC towards the end of our period of audit examination. To date, the Deputy Minister of DFAIT has chosen to delegate privacy responsibilities for PPTC to the Director of ATIP at DFAIT under section 73 of the *Privacy Act*. The ATIP Director works out of the DFAIT HQ in Ottawa and must rely on PPTC ATIP staff at the Gatineau HQ for information on privacy issues involving the passport program.

3.130 Without this delegation of ATIP authority to the Coordinator at PPTC, Passport Canada is dependent on the ATIP section at DFAIT to carry out its key activities for the protection of personal information under the *Privacy Act,* within the passport program.

3.131 In our view, the complexity of the passport program and the amount of sensitive personal information should not be underestimated as to their inherent risk. These factors point to the need for PPTC to carefully coordinate, implement and monitor the handling of this core information asset. In our view, there would be a real advantage for PPTC to have its own fully delegated and in-house ATIP Coordinator. Specifically, such a unit would be closer to the pulse of the organization's ongoing activities and plans and to understanding its unique informational challenges and needs.

3.132 The lack of delegated authority, together with the lack of a CPO, has resulted in the dispersal and neglect of certain key privacy responsibilities for the passport program. For instance, our audit found several gaps in the coordination and implementation of privacy responsibilities between DFAIT and PPTC. For example, Info Source (the institutional listing of its information holdings) for PPTC records was found to be years out of date; a Privacy Impact Assessment (PIA) for a significant new outsourcing initiative involving

Canada Post Corporation had not been carried out prior to its implementation; knowledge of privacy and security issues on the part of employees who handle passport information was lacking in certain regards; privacy clauses in the wording of contracts, MOUs and information-sharing agreements with other organizations had not been fully considered; and a comprehensive privacy breach protocol had not been developed.

3.133 ***Recommendation: Passport Canada's CEO should seek approval from the Minister of DFAIT to name a Chief Privacy Officer (CPO) as responsible and accountable for leading and coordinating all privacy roles and related issues across the passport program. PPTC should also seek a full delegation of ATIP authority to manage all access to information and privacy matters related to the passport program.***

Management Response (Passport Canada): Agree. Passport Canada has created an ATIP division in January 2008 in preparation to receiving the responsibility and accountability for leading and coordinating access to information and privacy matters relating to the passport program. The intent is to seek full delegation in 2008-09 from the Minister of DFAIT to manage all ATIP matters once all resources and processes are available. In addition, Passport Canada will study the recommendation to name a Chief Privacy Officer.

3.134 **Reporting Privacy Breaches.** We found that PPTC has a policy and operating procedures for handling and reporting security incidents. The policy applies to all PPTC facilities at headquarters and at regional offices. However, PPTC's breach procedures do not include the systematic reporting of privacy breaches to PPTC HQ from DFAIT missions and from one of its receiving agents. Additionally, the security breach protocol does not require that the ATIP office at DFAIT and ATIP officials at PPTC be informed of privacy breaches or consulted for advice in such instances.

3.135 The PPTC agreement with Service Canada includes a requirement that SC "promptly notify PPTC of any unauthorized disclosure or use of personal information," while the agreement with Canada Post Corporation does not.

3.136 We were informed that some past breaches, which could have affected the protection of personal information, had, indeed, not been reported to PPTC HQ. 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.

3.137 Treasury Board Secretariat and our office have issued guidelines and advice on how to handle privacy breaches. The Treasury Board Guidelines for Privacy Breaches indicates that "It is important to involve the ATIP Coordinator and the Departmental Security Officer (DSO) to ensure that the privacy of individuals and the security of assets are taken into account in the resolution process."

3.138 ***Recommendation: PPTC should ensure that its protocols for reporting security incidents include all privacy breaches by officials involved in the passport program and encompasses not just its own employees, but also those of its domestic Receiving Agents (RAs) and consular partners abroad. The protocol should also analyze any such breaches to help prevent their recurrence and include procedures for notifying clients who have been affected by a privacy breach.***

Management Response (Passport Canada): Agree. In accordance with the Treasury Board's privacy breaches directive, Passport Canada is developing its own privacy breaches directive with implementation planned for 2008-09. When implemented, this directive will complement existing procedures for handling of IT security incidents. Consolidated ATIP and protection of personal information training will continue to be provided to all staff and will include an awareness program to ensure all employees are cognizant of the Privacy Breaches Reporting Directive and Guidelines and are aware of their individual responsibilities for the protection of personal information in their custody. In addition, Passport Canada and DFAIT will work together to facilitate successful implementation of passport related directives at Canadian missions abroad.

3.139 **Information-Sharing Agreements (ISAs).** Paragraph 8(2)(f) of the *Privacy Act* requires government departments to develop arrangements or agreements covering the sharing of any personal information with other government organizations at the international, or provincial level. Treasury Board Policy requires that departments develop written agreements that define the extent of the sharing and the controls that are in place to protect personal information, which are signed by the parties. The purpose of such agreements is to ensure that the personal information shared is properly used according to the stated purposes, and that it is adequately protected throughout its life-cycle.

3.140 TBS has worked with the Institute for Citizen-Centred Service to develop best practice guidelines for Government-to-Government Personal Information Sharing, which provide useful advice and ISA templates to assist government institutions in their work on such agreements. TBS offers other guidance that would apply to contracts and service agreements with third parties involving Canadians' personal information entitled: *Taking Privacy into Account Before Making Contracting Decisions.*

3.141 PPTC has various service and information-sharing agreements with DFAIT, RAs, federal government organizations, and provincial and territorial birth and death registries. Principal federal government partners include Citizenship and Immigration Canada, Correctional Service Canada, Department of Justice, Canada Border Services Agency, Royal Canadian Mounted Police and Canadian Security Intelligence Service.

3.142 We found that some of PPTC's information-sharing agreements were several years old and had not been updated recently to ensure that they reflect current practices and the most up-to-date privacy requirements. Several of these agreements also lacked key privacy clauses called for in Treasury Board guidelines relating to protecting personal information. These clauses should define, for instance, what personal information will be shared, the limits to the sharing arrangement, security controls, and the requirements for monitoring and auditing to ensure that passport information is secure and adequately protected throughout its life cycle.

3.143 In comparing the text of the two agreements PPTC signed with each of its receiving agents (Service Canada and Canada Post Corporation), the SC agreement includes a whole section on privacy, which the CPC one does not. The SC agreement also provides significantly more privacy and security restrictions to protect personal information than does the agreement with CPC.

3.144 A 2006 Audit Report by the Office of the Auditor General also called for an umbrella agreement between PPTC and DFAIT that would define their respective roles under the passport program, which had not been developed at that time. PPTC and DFAIT still have not signed such an umbrella agreement at the time of this audit.

3.145 ***Recommendation: All Memoranda of Understanding (MOUs), agreements and other arrangements involving the sharing of personal information between PPTC and its partners should be updated in the near future to ensure that they reflect current practices and comply with all Treasury Board privacy, security and contracting requirements.***

> **Management Response (Passport Canada):** Agree. Passport Canada is committed to strengthening existing information sharing arrangements as well as exploring areas where future collaboration would contribute to advancing its mandate. Memorandum of Understanding negotiation process is complex and subject to resource availability at Passport Canada and within partner agencies. Passport Canada will review its existing agreements to identify areas where MOU enhancement in respect to current security and privacy requirements would be required and will engage with stakeholders as required.

3.146 **Privacy- and Security-Awareness Training.** Protecting personal information across an organization such as PPTC is of utmost importance. Employees who routinely handle Canadians' sensitive personal information as part of their duties must clearly understand their responsibilities for ensuring the protection of this information under the *Privacy Act*, and also have a sound grasp of their basic security responsibilities under the Government Security Policy.

3.147 To this end, government employees should receive ongoing privacy- and security-awareness training and updates. Such training would include defining individual roles and responsibilities for protecting personal information from inappropriate access, use, disclosure, modification or destruction. It would also cover other topics such as limiting the collection of personal information and the rights of individuals to access and correct their own personal information.

3.148 During our audit examination, we generally found that most PPTC program, DFAIT consular and Receiving Agent employees were aware of the confidentiality provisions in the *Privacy Act*. However, we also found that awareness was limited in other areas of privacy and informational security. The majority of staff interviewed during our audit could not recall having received privacy training or recent information security training.

3.149 For example, many DFAIT employees interviewed at diplomatic missions were not aware of the level of their personnel security clearance. Nor were most employees at PPTC and DFAIT aware that storing information such as passport applications, passports and original identity documents on open shelves or bins could present a privacy and security risk in terms of possible inappropriate access to this sensitive personal information.

3.150 In several instances, employees inappropriately disposed of certain passport forms containing personal information in regular garbage or recycling containers. When informed of these situations, employees did not appear to be aware that the discarded documents contained 'personal information' as defined by the *Privacy Act*.

3.151 We also noted that in certain consular areas abroad, mission staff—including Canadian-based and locally engaged staff—did not clearly understand the security risks and internal policies governing the use of electronic devices such as cell phones, memory sticks and BlackBerries at their missions. Some staff members indicated that they were allowed to bring them into consular areas, while others said they were not.

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

3.153 PPTC began a privacy training program for its operational staff and management as of December 2007. Having reviewed the training material provided by PPTC and DFAIT, we found that it was comprehensive and well-presented.

3.154 ***Recommendation: In order for employees to fully understand what they must do on a day-to-day basis, and to ensure that personal passport information is protected at all times, both PPTC and DFAIT should continue to use their privacy and security resources to deliver coordinated privacy and security training programs and related educational materials to PPTC employees domestically and consular officials abroad.***

Management Response (DFAIT): Agree. Reference is made to government employees to receive ongoing privacy and security awareness training. As part of the two week Consular Specialist training, LES employees (60-80 students per year) attend this course. As of September a module on the Security of Information will be included in this training course. DFAIT offers a half-day Security of Information course a number of times a year. A representative from the DFAIT Access to Information and Privacy Office participates at these courses to provide expert advice and respond to questions from participants. DFAIT also identifies, in its mandatory Introduction to Security course, the various levels of classified and protected information and the appropriate manner in which to safeguard sensitive information. DFAIT will be introducing a new on-line security course in the fall of 2008 which will serve to reinforce good security practices and will be required periodically by all employees. ATIP is working towards introducing a permanent Policy and Training capacity that will ensure that departmental-wide ATIP Awareness Training will be provided to all DFAIT officials on a regular basis, including the implementation of an on-line ATIP tutorial to reach DFAIT employees abroad. In addition, ATIP will work closely with the Information Management and Security Divisions to ensure a coordinated training approach as it relates to not only privacy but security and confidentiality of personal information as well.

Management Response (Passport Canada): Agree. Passport Canada will continue to work with internal and external partners to develop, deliver and monitor security and privacy training. A specific training course on the protection of personal information was developed by Passport Canada in 2007 and it is provided on an ongoing basis to all employees. Where feasible and beneficial, multi disciplinary approach will be used to develop and coordinate delivery of privacy and security related programs and awareness material.

3.155 **Other issues** – Please see Appendix B for a list of other privacy issues raised during the audit.

About The Audit

Audit Objective

The objective of this audit is to gather reasonable assurance that the personal information of Canadians and residents of Canada handled by PPTC and its partners is being adequately protected throughout its life cycle and to suggest improvements to the privacy and security management framework and processes at PPTC and its partners throughout the passport system.

Audit Mandate

The Office of the Privacy Commissioner of Canada (OPC) has the mandate to conduct compliance reviews (Audits) under section 37(1) of the *Privacy Act* with regards to the personal information handling practices of federal government institutions such as Passport Canada (PPTC) and the Department of Foreign Affairs and International Trade (DFAIT).

Audit Scoping

4.1 Our audit began with a survey or scoping exercise to identify those areas of the passport program of greatest potential risk to the privacy of Canadians. During this phase of the audit, the audit team reviewed publicly available documents about PPTC, and examined OPC complaint investigation and Privacy Impact Assessment (PIA) files, and reports from other oversight bodies such as the Office of the Auditor General. We also reviewed numerous PPTC program and DFAIT consular policies and procedures relating to passport operations.

Audit Examination

4.2 The audit examination field work consisted of visits to: PPTC's principal passport-printing centres in the National Capital Region and Greater Toronto Area; call centres in the NCR and Montreal; Canada Post Corporation and Service Canada (Receiving Agent) service locations at headquarters and in the Quebec/Atlantic, GTA and Western Regions.

4.3 Facilities examined included public waiting areas at service locations, service counters, processing areas, records-storage facilities, locations where records were destroyed, and IT server rooms.

4.4 Similar audit activities took place at DFAIT missions abroad in Berne, Paris, Beijing, Los Angeles and Taipei, where we reviewed the delivery of passport services within the "Consular Services" areas of these missions. We also inquired about the role of Honorary Consuls who provide emergency travel document services to Canadians at more than 100 locations abroad.

4.5 In addition, we examined various corporate functions at PPTC and DFAIT that support the passport program. These functions included privacy activities within the ATIP

Secretariat, and physical, personnel and IT security functions. We also reviewed information-sharing arrangements between PPTC and its partners, investigations and intelligence functions, and the training activities for employees related to privacy and security.

4.6 We augmented the above audit examination work with a detailed review of background documents, written queries to relevant officials, and many structured interviews in every program area, activity and facility examined.

4.7 Although Members of Parliament do assist constituents with passport applications, these activities were not within the scope of our audit; Parliament falls outside of the OPC's mandate.

4.8 The OPC audit team received exceptional cooperation from PPTC and its partners throughout our audit, despite heavy work demands and other competing operational pressures. Full and timely access to information, documentation, facilities and personnel was provided as requested.

4.9 Our audit examination field work was substantially completed by January 31, 2008.

Audit Methodology

4.10 Our audit methodology combined a number of approaches. It began by establishing audit criteria through a review of legislation, regulations, Orders in Council, Treasury Board Secretariat and government policies and guidelines. We also compared operational policies, practices, agreements, contracts and training materials against established privacy audit criteria.

4.11 File and document reviews were conducted to understand the quality control, intelligence and investigation functions at the Security Bureau of PPTC.

4.12 The audit team also conducted a walk-through of facilities to observe the handling, storage and physical security of documents. In addition, we witnessed several live demonstrations of IT systems at PPTC and DFAIT to observe how personal information was collected, used, shared and disclosed through both organizations' electronic systems.

4.13 Finally, OPC hired an outside contractor to carry out an evaluation of PPTC's public website, with a special emphasis on the security and privacy controls it uses.

Audit Criteria

4.14 At the outset of the audit, the audit team expected PPTC and its partners' management of Canadians' personal information to:

- Comply with the obligations of the Canadian Passport Order as amended;
- Comply with sections 4 to 8 of the *Privacy Act*;
- Respect applicable Treasury Board and Government of Canada policies; and
- Observe the ten internationally recognized fair information principles set out in *Personal Information Protection and Electronic Documents Act*.

Note: *Please see Annexes C and D for our audit lines of enquiry and detailed audit criteria. Lines of enquiry and audit criteria were shared with PPTC and the OPC received confirmation of their acceptance as the basis of our audit examination.*

Audit Standards

4.15 The audit work reported here was conducted in accordance with the legislative mandate, policies, and practices of the Office of the Privacy Commissioner of Canada. These embrace the standards recommended by the Canadian Institute of Chartered Accountants (CICA).

Audit Team

Trevor R. Shaw, CA CMA
Acting Director General Audit and Review

Raymond Brault
Senior Audit and Review Officer

Tom J. Fitzpatrick
Manager Audit and Review
& Audit Lead

William Wilson
Audit and Review Officer

Annex A – List of Audit Recommendations

Collection of Personal Information

1. PPTC should explore options as to the best method of collection of financial information about applicants and guarantors personal data that does not unduly impede the passport process, while considering the privacy of these individuals. It should also revise training and policy documents to limit the collection of the SIN, while actively encouraging applicants to use other forms of identification that pose less privacy risk.

Controlling Access, Use and Disclosure of Personal Information

2. PPTC and DFAIT should jointly take steps necessary to control employees' access to personal information. These steps should reflect its Protected-B classification, follow the need-to-know principle, and involve implementing electronic audit trails for IRIS and PMP systems to minimize the risk of inappropriate access to personal information.

Ensuring Proper Retention and Disposal of Personal Information

3. Given the risks inherent in retaining passport information for a 100-year period, and considering the requirements of the *Privacy Act* to retain personal information only for as long as necessary or as defined in regulations, PPTC should consult with Library and Archives Canada to reassess this exceptionally long records-retention period.
4. PPTC should assess the privacy and security risks relating to its current practices for disposing and/or destroying sensitive personal information for all types of records.

Providing Essential Safeguards

5. **Physical Security.** PPTC and DFAIT should ensure that paper-based files containing passport information are stored in a manner appropriate for particularly sensitive Protected-B information according to the *Government Security Policy*.
6. PPTC and DFAIT should review physical and other safeguards to ensure that only persons who have an operational need to enter areas where passports are processed are allowed to do so.
7. PPTC and DFAIT should review the layout and acoustics of all public service locations to ensure that they provide an adequate level of privacy for their clients through appropriate sight and sound barriers and signage.
8. **Personnel Security Screening.** PPTC and DFAIT should ensure that all employees and contractors handling passport information have adequate personnel security clearances, as required by the *Government Security Policy* and Treasury Board Policy. Any contractors, cleaning staff or visitors lacking security clearances should be escorted at all times by a PPTC or DFAIT employee.
9. Where it is impossible to obtain equivalent personnel security clearances for Locally Engaged Staff at missions, DFAIT should place increased reliance on access controls and audit trails.

10. **IT Security.** PPTC and DFAIT should develop a policy limiting the use of portable memory and recording devices on their premises, and explore the feasibility of controlling the ability of staff to connect these devices to internal information systems. Employees should be informed of this policy and notices should be posted at main entrances to passport processing areas. In addition, periodic sweeps should be carried out to ensure that this policy is respected.
11. PPTC and DFAIT should consider encrypting all passport information stored on the IRIS and PMP systems to better protect it from inappropriate access, and develop strategies for ensuring that all e-mails containing personal information that are sent outside of secure networks are encrypted or otherwise sent by a secure means.

Building a Privacy and Security Management Framework

12. **Accountability for Privacy.** Passport Canada's CEO should seek approval from the Minister of DFAIT to name a Chief Privacy Officer (CPO) as responsible and accountable for leading and coordinating all privacy roles and related issues across the passport program. PPTC should also seek a full delegation of ATIP authority to manage all access to information and privacy matters related to the passport program.
13. **Privacy Breaches.** PPTC should ensure that its protocols for reporting security incidents includes all privacy breaches by officials involved in the passport program and encompasses not just its own employees, but also those of its domestic Receiving Agents (RAs) and consular officials abroad. The protocol should also analyze any such breaches to help prevent their recurrence and include procedures for notifying clients who have been affected by a privacy breach.
14. **Information-Sharing Agreements.** All Memoranda of Understanding, agreements and arrangements involving the sharing of personal information between PPTC and its partners should be updated in the near future to ensure that they reflect current practices and comply with all Treasury Board privacy, security and contracting requirements.
15. **Privacy- and Security-Awareness Training.** In order for employees to fully understand what they must do on a day-to-day basis, and to ensure that personal passport information is protected at all times, both PPTC and DFAIT should continue to use their privacy and security resources to deliver coordinated privacy and security training programs and related educational materials to PPTC employees domestically and consular officials abroad.

Annex B – Other Audit Issues

The following issues stem from our audit examination work and analysis, with respect to the personal information management practices at PPTC, DFAIT missions ("Consular Services") and Receiving Agents (RAs). Many of these issues are related to the recommendations found in the main body of the audit report.

Ensuring Proper Retention and Disposal of Personal Information

- Credit card information currently collected along with passport applications is retained for a period of time beyond what is necessary for passport program needs.
- Completed passport application documents at PPTC and DFAIT are not tracked until their destruction to ensure that they do not go missing while in storage and that they are destroyed when no longer needed.
- Some Honorary Consuls abroad make unnecessary copies of passport applications and statutory declarations.
- DFAIT has not developed a common retention and disposal schedule for Closed Circuit Television (CCTV) images recorded in consular areas to ensure that these records are not retained any longer than necessary.
- In some public waiting areas, secure facilities are unavailable to the public to dispose of partially completed passport applications containing personal information.

Providing Essential Safeguards

- **Computer Monitors.** At a few PPTC locations visited during the audit, the position of computer monitors used by passport officers allowed the public or other unauthorized persons to view sensitive personal information.

  Note: *The following comments are based on a scan of the PPTC public website carried out in 2007 by an outside contractor Watchfire.*

- **PPTC Website (www.ppt.gc.ca).** The on-line "Complaint to Ombudsman" and "Feedback Questionnaire" forms (English and French versions) were found to be unencrypted on the PPTC website.
- The "auto-complete" browser function was not disabled for all online forms unprotected by epass.
- Notification of all *Privacy Act* rights were not provided on all PPTC on-line forms collecting personal information.
- No notice is provided advising users when they are leaving the secure PPTC website and entering a third-party site, which may not have the same security features.

Building a Privacy and Security Management Framework

- PPTC is not receiving Threat and Risk Assessments (TRAs) from Receiving Agents (RAs), as required by contract for its review.
- **Privacy Impact Assessments.** Not all PPTC PIA and preliminary PIA summaries are posted on its website as required by the TBS policy on PIAs.
- **Privacy Notices.** PPTC passport forms' privacy notices do not inform applicants of their rights of access, correction and complaints relating to their personal information.

Annex C – Lines of Enquiry and General Audit Criteria

LINES OF ENQUIRY & GENERAL AUDIT EXAMINATION CRITERIA	OBSERVATIONS & FINDINGS)
LINE OF ENQUIRY 1: COLLECTION OF PERSONAL INFORMATION *Does it appear the collection of personal information is performed in a safe and secure manner and is limited to the purposes of passport issuance?* (*Privacy Act, Sections 4, 5 and 7*)	
Is the personal information collected limited to the purposes of passport issuance and with the consent of the applicant?	
- Personal information collected is used only to make the determination of entitlement and subsequent issuance of a passport.	
- Personal information collected is done with the informed consent of the applicant.	
Is the personal information collected in a 'safe and secure' manner? (i.e. Government Security Policies & MITS Standard*)*	
- The location and method of collection is performed in a safe and secure environment.	
- The personal information is maintained in a safe and secure environment.	
- The transport and transmission of personal information is done in a safe and secure manner.	
Are adequate controls and measures in place in order to safeguard the collection of personal information?	
- The collection of personal information is governed by prescribed procedures.	
- The prescribed procedures are followed by the collecting unit.	
- The collection activities involving personal information are monitored and reviewed on an ongoing basis in order to identify and mitigate privacy risks.	
LINE OF ENQUIRY 2: USE OF PERSONAL INFORMATION Does it appear the use of personal information is conducted in a safe and secure manner and is limited to the purposes of passport issuance? (*Privacy Act*, Sections 4 and 7)	
Is the use of the personal information limited to the purposes of passport issuance or as prescribed by law?	
- Personal information is used only to make the determination of entitlement and subsequent issuance of a passport or as prescribed by law.	

LINES OF ENQUIRY & GENERAL AUDIT EXAMINATION CRITERIA	OBSERVATIONS & FINDINGS)
While being processed, is the personal information maintained in a safe and secure manner?	
- The location used to process applications is a safe and secure environment.	
- The personal information is stored in a safe and secure environment.	
- The transport and transmission of personal information is done in a safe and secure manner.	
Are adequate controls and measures in place in order to safeguard personal information?	
- The processing and use of personal information is governed by adequate prescribed procedures, which are followed by the processing unit.	
LINE OF ENQUIRY 3: DISCLOSURE OF PERSONAL INFORMATION Is personal information being disclosed without consent beyond permissible exceptions*?* (Section 8 *Privacy Act*)	
Does Passport Canada share personal information with domestic and/or foreign agencies?	
- All such information sharing is permitted by law.	
- Adequate controls and agreements are in place for each information sharing arrangement	
Are adequate access and control mechanisms in place to prevent the unauthorized disclosure of personal information?	
- Access to personal information is limited to a 'need-to-know' basis.	
- All disclosures to third parties are documented.	
- Adequate controls are in place to prevent disclosure of personal information to anyone other than the applicant or authorized users.	
- The processing and disclosures of personal information is monitored and reviewed on an ongoing basis in order to identify and mitigate privacy risks.	
LINE OF ENQUIRY 4: RETENTION AND DISPOSAL OF PERSONAL INFORMATION *Does it appear personal information is retained for the appropriate period and disposed of in an appropriate manner?* (*Privacy Act, Section 6*)	
Is the information retained only for an appropriately prescribed period?	
- There is a prescribed period for which the data is retained.	

LINES OF ENQUIRY & GENERAL AUDIT EXAMINATION CRITERIA	OBSERVATIONS & FINDINGS)
- What is the disposal schedule for rejected passport applications?	
- The data is disposed of at the end of the retention period.	
Is the information disposed of appropriately?	
- There is a prescribed and secure method of disposal for the information that is followed.	
LINE OF ENQUIRY 5: PRIVACY MANAGEMENT FRAMEWORK *Does it appear that an effective Privacy Management Framework or administrative infrastructure is in place to support the processing and issuance of passports?* (*Privacy Act, Section 2 and Principle 1 Accountability of* PIPEDA)	
Has PPTC designated an individual or individuals who are accountable for the organization's compliance with privacy obligations?	
- Specific privacy-related accountabilities are established within the institution.	
- The organizational structure for privacy-related processes is formally and effectively supported.	
- Privacy-related policies, regulations and guidelines are identified, evaluated and incorporated into operational activities.	
- Have employees been trained on an ongoing basis about their privacy and security obligations and rights?	
- Objectives and goals of privacy-related processes are clearly defined, formally approved and effectively communicated.	
- Control activities and mechanisms for privacy-related processes are in place, relevant, comprehensive and address known risks.	
- The organization has established adequate safeguards for personal information transferred to third parties including adequate contracts and agreements and effective oversight.	

Annex D – Detailed Audit Criteria

Note:

The evaluation criteria for this audit are derived principally from obligations set out in sections 4 to 8 of the *Privacy Act*, the Government Security Policy, Treasury Board policies, guidelines and related documents governing the management of personal information.

In addition, some best practices criteria have also been adapted from Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).

Accountability (Principle 1 PIPEDA):

Criteria:

- The organization must designate individual(s) who will oversee and coordinate the organization's activities to ensure the accountability for the organization's compliance with all privacy obligations.
- Those individuals may delegate specific roles and responsibilities across the organization for ensuring privacy and security protections of its personal information holdings.
- The organization shall: use contractual or other means to ensure that third parties provide a comparable level of privacy protection as does the originating organization.

  Note: *Reference is made to criteria for information sharing agreements and contracting out. For information held by a government institution, the standard would have to be as good as or better than that provided by the Privacy Act, Government Security Policies and TB Guidelines.*
- Organizations shall: implement policies and practices to give effect to the principles, including procedures to protect personal information; establish procedures to receive and respond to complaints and inquiries; train staff and communicate to staff information about the organization's policies and practices; and develop information to explain the organization's policies and procedures.

  Note: *See also TBS "Roles and Responsibilities" under the Privacy and Data Protection Policy for specific requirements related to a Privacy Management Framework.*

Notification of Purposes (subsection 5(3) of the *Privacy Act*):

Criteria:

- Subject to exceptions referred to in subsection 5(3) of the *Privacy Act*, government institutions are required to inform individuals of the purpose for which the information is being collected and the intended uses to be made of it.

Identifying Purposes (Principle 2 PIPEDA):

Criteria:

- The organization shall document the purposes for which personal information is collected.
- The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.
- When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.
- Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

  Note: *There may be exceptions to this principle, where the collection is done according to law and information provided to the individual may result in less or inaccurate personal information being collected.*

Collection of Personal Information (Sections 4 and 5 of the *Privacy Act):*

Criteria:

- Government institutions shall collect personal information only when it relates directly to an authorized program or activity of the institution.
- Wherever possible, government institutions shall collect personal information – intended to be used for an administrative purpose – directly from the individual to whom it relates.

Consent (Principle 3 PIPEDA)

Criteria:

- Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Limiting Collection (Principle 4 PIPEDA):

Criteria:

- Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.
- Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the openness principle. (Principle 8 of PIPEDA also refers to this).

  Note: *See also, TBS Guidelines on 'Collection of Personal Information'.*

Use of Personal Information (Subsection 6(2), section 7 and subsection 9(4) of the *Privacy Act)*:

Criteria:

- Government institutions shall take all reasonable steps to ensure that personal information that is used for an administrative purpose is as accurate, up-to-date and complete as possible. (See also Accuracy – Principle 6 of PIPEDA)
- Without the consent of the individual to whom it relates, personal information shall only be used by a government institution for the purpose for which it was collected, or for a use consistent with the original purpose, or for a purpose for which the information may be disclosed within or outside the institution under subsection 8(2) of the *Privacy Act*.
- When personal information is put to a consistent use that is not listed in the personal information bank description in *Info Source*, such a use must be reported to the Privacy Commissioner and included in the next statement of consistent uses set out in *Info Source*.

  Note: *See also, TBS guidelines for the 'Use and Disclosure of Personal Information'.*

Limiting Use, Disclosure and Retention (Principle 5 PIPEDA):

Criteria:

- Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
- Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods.
- Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made.
- Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous.
- Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

Use – Data Matching (Treasury Board Policy on Data Matching):

Criteria:

- Government institutions must ensure that their data matching programs are designed and conducted in accordance with the principles of fair information practices embodied in the *Privacy Act* and in compliance with the Treasury Board Policy on Data Matching.

Disclosure of Personal Information (Section 8 of the *Privacy Act*):

Criteria:

- Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed to a third party except in the limited number of circumstances established in subsection 8(2) of the *Privacy Act*.

Disclosure – Contracting Out (Criteria developed by the OPC):

Criteria:

- Personal information which is collected, used, processed, disclosed, held or disposed of on behalf of a government institution, or in fulfillment of a contract with a government institution, shall be managed in conformity with the principles of fair information practices embodied in the *Privacy Act* and the *Privacy Act Regulations.*
- When a private sector agency or contractor manages personal information on behalf of a government institution, the contract must specify that such personal information is deemed to be under the control of the government institution and is subject to the *Privacy Act.*
- The contract must also stipulate, where applicable, how the service provider or contractor will meet the *Privacy Act*'s requirements in terms of managing the personal information it will handle while carrying out the contract.
- The contract should also recognize the Privacy Commissioner's right of access to the personal information for the purposes of conducting audits and investigations.

Retention and Disposal (Subsections 6(1) and 6(3) of the *Privacy Act* and paragraphs 4(1) and (2) and section 7 of the *Privacy Act Regulations*):

Criteria:

- Personal information must be retained and disposed of in accordance with approved records retention and disposal schedules.
- Except as otherwise provided in law or where the individual consents to earlier disposal, personal information that has been collected for an administrative purpose – that is, in the decision-making process that directly affects the individual – must be kept for a minimum of two years after the last time it was so used.
- Records should be properly disposed of in a manner consistent with their security classification.

Accuracy (Subsection 6(2) of the *Privacy Act*):

Criteria:

- A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

Accuracy (Principle 6 PIPEDA):

Criteria:

- Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
- An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purpose(s) for which the information was collected.

Safeguarding Personal Information (Sections 6, 7 and 8 of the *Privacy Act*):

Criteria:

- Government institutions must have in place appropriate security measures to ensure that, throughout its life cycle, personal information under their control is protected and not vulnerable to unauthorized access, use, disclosure, alteration or destruction.

E-mail & Facsimiles:

Criteria:

- Identifiable personal information should not be sent by e-mail or fax, unless by secure means (e.g., encrypted message, secure fax in a secure area).

  Note: *There are many reasons why sending personal information by e-mail or fax poses security risks. If sent or received by insecure means, the information may be intercepted or exploited, or received in error by someone who is not authorized to receive the information.*

Safeguards (Principle 7 PIPEDA):

Criteria:

- Security safeguards must be adequate to protect personal information against loss or theft, as well as unauthorized access, disclosure, use, modification or reproduction.
- Organizations shall protect personal information regardless of the format in which it is held.

  Note: *The nature of the safeguards will vary depending on the sensitivity and amount of personal information collected, its distribution, the format of the data and the method of storage.*
- The methods of protection should include adequate: physical measures (e.g., locked filing cabinets and restricted access to offices); organizational measures (e.g., security clearances); and technological safeguards (e.g., the use of passwords and encryption to protect personal information).
- Access rights to personal information should be determined on a ‘need-to-know basis’.

  Note: *The nature of appropriate safeguards varies with the sensitivity of information, the amount, distribution and format of the information and the method of storage.*
- Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.
- Care shall be exercised in the disposal or destruction of personal information to prevent unauthorized access to it.

Access (Sections 12 to 28 of the *Privacy Act*):

Criteria:

- Government institutions must provide citizens and persons residing in Canada with access to their personal information, when a written request has been received from the individual, within the time frames specified in the *Privacy Act* and subject to exemptions set out in sections 18 to 28 of the *Privacy Act*.
- Access may be provided by permitting the individual to examine the information or by providing the individual with a copy thereof.
- Where access is refused, the institution shall notify the individual that the information does not exist or state the specific exemption provision of the *Privacy Act* upon which the refusal was based. The individual must at the same time be advised of their right of complaint to the Privacy Commissioner for refusal.

Access (Principle 9 PIPEDA):

Criteria:

- Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information.
- An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.
- In providing an account of third parties to which it has disclosed personal information, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.
- Where personal information has been transferred to a third party contractor, the organization must ensure that it obtains copies of records relevant to the access request from the third party.
- Where personal information has been disclosed under an information sharing agreement, the organization must ensure that it keeps the originals for any access requests for these records.
- An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.
- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. The amendment may involve the correction or deletion of information, or the inclusion of additional information. Where appropriate, the amended information shall be transmitted to third parties having access to the information at issue.

Complaints (sections 29 and 34 of the *Privacy Act*):

Criteria:

- Institutions must cooperate with the Privacy Commissioner in their investigation of complaints from the public, or self initiated complaints by the Privacy Commissioner under the *Privacy Act*.
- Institutions must allow their officials to give oral or written evidence to the Privacy Commissioner.
- Institutions must allow the Privacy Commissioner's delegated officials to enter any premises occupied by any government institution on satisfying any security requirements of the institution related to the premises.
- Institutions must allow the Privacy Commissioner's delegated officials to converse in private with any person on any premises occupied by a government institution within the authority of the Privacy Commissioner under the *Privacy Act* as the Commissioner sees fit.
- Institutions must allow the Privacy Commissioner's delegated officials to obtain copies of or extracts from books or other records found in any premises entered containing any matter relevant to the investigation.
- Institutions must allow the Privacy Commissioner's delegates access to any information except confidences of the Queen's Privy Council for Canada (Subsection 70(1) of the *Privacy Act*).

Challenging Compliance (Principle 10 PIPEDA):

Criteria:

- An individual shall be able to address a challenge concerning compliance with the principles (Schedule 1 to PIPEDA) to the designated individual or individuals accountable for the organization's compliance.
- Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
- Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant redress procedures (including the right of complaint to the Office of the Privacy Commissioner of Canada).
- An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

OTHER AUDIT CRITERIA

Awareness of the *Privacy Act:*

Criteria:

- Government employees handling personal information must be aware of their obligations under the *Privacy Act,* including restrictions on disclosures of personal information.
- The government institution must provide employees with appropriate *Privacy Act* training and documentation to ensure that they are kept up-to-date on their privacy obligations.

  Note: *Compliance with the spirit and specific requirements of sections 4 to 8 of the Privacy Act depends largely on the degree of understanding of the provisions of the Privacy Act by the persons responsible for administering the Privacy Act for the institution and, to a lesser degree, by other employees of the institution. The accountability principle 1 in* PIPEDA *contains similar provisions.*

Info Source (Sections 9, 10 and 11 of the *Privacy Act*)

Criteria**:**

- Government institutions must ensure that all such descriptions are as complete, up-to-date and accurate as possible.

  Note: *As a complement to sections 4 to 8 of the Privacy Act, sections 9, 10 and 11 of the Privacy Act require that all personal information holdings must be described and published in Info Source as Personal Information Banks or as classes of personal information.*

Annex E – Summary of Passport Information Systems

Note: *PPTC stores and manages the personal information in three personal information banks (PIBs) shown hereunder:*

Personal Information Banks (PIBs)	Information Holdings
Regular and Official Travel Passports	IRIS PMP Microfilm
Certificates of Identity and Refugee Travel Documents	IRIS Microfilm
System Lookout Files	IRIS ForeMost CSC Secondary Storage C-41 Interface Security Files

Integrated Retrieval Information System (IRIS): PPTC's main electronic passport issuing system, which is used to manage passport entitlement and production.

IRIS is an integrated system comprising of the following electronic databases:

- **Central Index (CI)**: master index of passport records, which includes digitized images of passport application forms and supporting documentation.
- **Passport On-line (POL):** database containing passport application information submitted by members of the public over the Internet using Government-on-line/Secure Channel.
- **Work in Progress (WIPs)**: databases used to process and store passport applications; data is transferred to the Central Index post-production (i.e. after passports are issued).
- **System Lookout (SL)**: database containing index biographic details (names, date of birth) on individuals whose passport entitlement may require further review or investigation under the *Canadian Passport Order*.

Passport Management Process (PMP) system: DFAIT's passport component of the COSMOS IT system, which contains the integrated consular system. PMP is used to record and process passport applications and supporting documents abroad. The data is copied to the PPTC Central Index system (CI) in Canada after the passport is issued abroad.

Microfilm: Copies of passport applications and supporting documents were maintained on microfilm for applications made prior to 2002 at which time the IRIS system was created.

CSC Secondary Storage: Electronic database containing personal information obtained from Correctional Service Canada (CSC) on offenders and parolees regarding individuals on the PPTC System Lookout (SL) database.

C-41 Interface: Electronic database containing personal information obtained from the Department of Justice Canada for use in administering the *Family Orders and Agreement Enforcement Assistance Act* (Bill C-41) – individuals on the System Lookout (SL) database.

Security Files: Paper files containing supplementary passport entitlement and case management information – individuals on the System Lookout (SL) database, which is accessed by a small number of officials at the PPTC Security Bureau.

ForeMost: Electronic records management system used to retain corporate records, including electronic documents, including individuals on the System Lookout database.