Public Safety Canada | Sécurité publique Canada

Public Safety Canada
Internal Audit of the Management Control Framework over Personal Information

September 2015

Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

Public Safety Canada ("PS" or "Department") provides strategic policy advice and support to the Minister of Public Safety and Emergency Preparedness on a range of issues, including: national security, border strategies, countering crime and emergency management. The Department also delivers a number of grant and contribution programs related to emergency management, national security, and community safety. The Department also coordinates the efforts of PS's portfolio agencies as well as provides guidance on their strategic priorities. Portfolio agencies are more operational in nature, and include the Canada Border Service Agency (CBSA); Canadian Security Intelligence Service (CSIS); Correctional Service of Canada (CSC); Parole Board of Canada (PBC); and the Royal Canadian Mounted Police (RCMP).

PS is subject to the *Privacy Act*, and must adhere to its requirements related to the management and safeguarding of personal information. The *Privacy Act* defines personal information broadly as "*information about an identifiable individual that is recorded in any form*". The *Privacy Act* protects the privacy of all Canadian citizens and permanent residents of Canada regarding personal information held by a government institution against unauthorized use and disclosure. The *Privacy Act* also gives Canadians, the right to access personal information held by the government. The Treasury Board Secretariat (TBS) has also implemented privacy-related policies and directives that provide additional requirements on the collection and management of personal information, including the *Policy on Privacy Protection*, *Directive on Privacy Impact Assessments* (PIA), and *Directive on Privacy Practices*.

Given the Department's role in policy coordination and advice, it does not collect a significant amount of personal information directly from the public, with only a small number of activities identified through the audit that collect and manage citizen-related personal information. Departmental employee information represents one of, if not the largest, personal information holdings within the Department, in relation to the management of human resources.

Although the Department does not manage a significant number of personal information holdings, what is does manage is often sensitive in nature. A privacy breach within the Department (i.e., unauthorized access to, or collection, use, disclosure, retention, or disposal of personal information) could have serious consequences for the reputation of PS, and may have operational impacts such as impeding the Department's ability to gain access to needed research data. Furthermore, given the Department's coordination and support role within the PS Portfolio, as well as outreach to other jurisdictions and stakeholders involved in public safety, any reputational harm may have serious impacts to the Government as a whole. Furthermore, a breach may result in departmental resources being required to investigate and respond to the breach, including addressing enquiries or audit activities from the Office of the Privacy Commissioner (OPC).

Audit Objective and Scope

The objective of the audit was to provide reasonable assurance that the Department's Management Control Framework over the management of personal information is adequate and effective to ensure that the Department is in compliance with the *Privacy Act* and both Treasury Board Secretariat and PS related policies.

The scope of the audit, which covered the period ending April 30th 2015, was to examine the accountability and policy framework as well as key procedures and other controls that are in place to:

- Ensure compliance to the *Privacy Act*, the TBS and PS associated policies;
- Define and communicate requirements in this area;
- Ensure an efficient and effective response to these requirements; and,
- Safeguard the Department's reputation and credibility as it relates to the Department's management of personal information.

Based on the audit's planning phase, the scope of the audit focused on a review of the PS Privacy Management Framework (PMF) and its application on selected personal information holdings. During the planning phase, personal information holdings across the Department related to both PS employees and the public, in both electronic and hardcopy format, were determined and based on those planning activities, those areas with personal information holdings selected for further examination include:

- Emergency Management and Programs Branch (EMPB);
- Community Safety and Countering Crime Branch (CSCCB);
- National and Cyber Security Branch (NCSB); and,
- Corporate Management Branch (CMB).

The audit's scope included personal information holdings related to both PS employees and the public, in both electronic and hardcopy format.

Summary of Findings

The audit team observed examples of how controls are properly designed and applied effectively. This resulted in several observed strengths:

- At an overall level, the Department has ensured it has appropriate "incident management" practices in place in the event of a privacy breach, including the development and implementation of privacy breach management policies and processes. It should also be noted that, for the privacy breaches brought to the attention of the Access to Information and Privacy (ATIP) Division, the audit team found that they were handled and followed-up on in an appropriate fashion.
- A policy and processes for the completion of PIAs has been implemented, and those PIAs reviewed as part of the audit were completed and managed in an appropriate manner.
- The Department has defined delegation of authorities for the *Privacy Act*, and ATIP Division roles and responsibilities are clearly defined for activities within their directorate.

- It was noted that two positions have recently been staffed (September 2014) within the ATIP Division to focus on the further development and implementation of access to information and privacy policies and training/awareness activities, which is a critical component of a privacy program.
- Departmental employees encountered through this audit demonstrated an appreciation for the importance of safeguarding personal information.

Within the existing PMF the audit identified areas where management practices and processes could be improved to reduce the risk of a privacy breach, as summarized below:

Departmental Privacy Management Framework (PMF)

While the Department has a Privacy Management Framework (PMF) in place, it is still evolving and continues to mature, and some gaps were noted through the conduct of the audit. At an overall level, the audit noted that the ATIP Division was not well integrated within the Department's business processes and the privacy roles and responsibilities of the ATIP Division versus other functional areas were not clearly defined or formally established. This has resulted in the ATIP Division not being consulted on a number of areas in which their input would have been appropriate, including the development of information sharing agreements that involve personal information. Furthermore, concerns were noted that program or functional areas may not recognize the ATIP Division as their first point of contact for privacy-related questions, and may instead consult with other groups (e.g., legal or security) within the Department or may seek advice directly from the OPC.

Within some of the program areas that were audited, personal information was collected and managed without a PIA being conducted or a formal assessment to determine if a PIA was required.

The audit noted that there were not established processes and metrics in place for the evaluation and measurement of the effectiveness of the implementation of the Department's PMF. Further the regular monitoring of personal information activities and breaches, while done, was not formalized.

Additionally, the ATIP Division's draft training plan could be improved through greater targeting of envisioned training to specific or higher risk program areas that collect and/or manage personal information.

Controls related to the Management of Personal Information

Although no major issues were noted with respect to how personal information was being collected, used, and disclosed in those areas that were included within the scope of the audit, the processes related to how personal information was managed by program areas have generally not been formally documented. Without formally documented guidelines and processes for the management of personal information, there is a risk that appropriate practices may not be followed, especially if there are changes in staff within the areas that manage personal information. Furthermore, formal standard operating procedures are critical to demonstrate to

stakeholders and the OPC that appropriate processes have been established and are available to support the Department should a privacy breach occur.

Additionally, it was noted that some functional areas had very long or undefined retention periods for files containing personal information.

Safeguarding of Personal Information

Based on the audit work performed, the main repositories for files containing personal information within PS are Records, Document and Information Management System (RDIMS), PeopleSoft, the network drive, portable storage and secure filing cabinets. While secure filing cabinets and PeopleSoft access was well controlled, audit testing revealed weaknesses in access controls related to RDIMS and network folders. Further it was noted that the Information Management function does not formally monitor incidents when excessive access it granted. Restricting access to personal information to the individuals that require access as part of their job duties helps mitigate the risk of a privacy breach.

Audit Opinion

PS has moderate issues related to the adequacy and effectiveness of the management control framework over personal information and compliance with the *Privacy Act* and TBS and PS related policies. There are opportunities for improving the management control framework over personal information to better identify risks and ensure appropriate monitoring to prevent and detect potential non-compliant activities.

This report and audit were conducted for PS management purposes. Use of this report for other purposes may not be appropriate.

Statement of Conformance and Assurance

The audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined.

Recommendations

1. The Assistant Deputy Minister Portfolio Affairs and Communications should develop and implement a formal plan, with defined timelines and accountabilities, to address the identified gaps in the Department's PMF. The plan should address:
   a. Defining roles and responsibilities related to privacy between functional areas as well as ensuring privacy considerations are embedded within business processes.

b. Formalizing the process for updating Personal Information Bank (PIB) entries and reviewing PIBs so that all personal information holdings used for administrative purposes within the Department have a corresponding PIB entry in InfoSource. The ATIP Division should initially undertake a more comprehensive PIB update process to ensure an inventory of all personal information holdings is documented within the Department. This should also consider those personal information holdings used for non-administrative purposes.
c. Establishing departmental policies and guidelines that specify privacy requirements for the development of information sharing agreements and contribution agreements.
d. Revising and executing on the training plan to target training to specific or higher risk program areas that manage personal information, and implementing on a timely basis. The ATIP Division should coordinate their planned training with the baseline training offered by the Canada School of Public Service. As part of the training, it should be reiterated that program areas managing personal information should consult the ATIP Division and consider the need to complete a PIA. In addition, program areas that were identified as collecting and managing personal information without completing a PIA should either complete a PIA or document a rationale for not doing so.
e. Establishing a monitoring program with related performance metrics for the evaluation and measurement of the privacy program's success, and presenting regularly to senior management (e.g. quarterly to the Departmental Management Committee) specifically on the status of key privacy matters.

2. Each Assistant Deputy Minister should formally document the processes for the collection, use and disclosure of personal information in those program areas that manage personal information. This should include clear guidelines related to the use of personal information so that there is a consistent understanding over what constitutes acceptable management and safeguarding of personal information.

3. Each Assistant Deputy Minister where applicable should review the retention periods for personal information to determine if the length of time is reasonable and ensure that these schedules are updated as required.

4. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch, where applicable should review the default access settings for documents in RDIMS that contain personal information. This should include the implementation of monitoring activities related to RDIMS access rights, and a process for follow-up and mitigation when excessive access rights are granted to documents containing personal information.

5. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch, where applicable should review any instances in which program areas are storing personal information on the Departmental network drives in order to:
   a. Determine if the use of the network drive for the storage of the personal information is appropriate;
   b. Review and ensure access is limited to only those individuals that have a requirement to access the information; and,

c. Based on the sensitivity of the personal information, determine if additional controls should be implemented (e.g., file encryption) given that personal information stored on network drives may be accessible by network administrators, including network administrators with Shared Services Canada (SSC).

Management Response

Management accepts the recommendations of Internal Audit and will work collaboratively to develop and implement applicable protocols and practices to effectively and adequately manage personal information to ensure that the Department is compliant with the Privacy Act, and both Treasury Board Secretariat policies and Public Safety Canada policies.

The key actions to be taken by management to address the recommendations and findings and their timing can be found in the Findings, Recommendations and Management Response section of the report.

CAE Signature

_____

Audit Team Members

Rosemary Stephenson
Denis Gorman
Deborah Duhn
With the assistance of external contractors

Acknowledgements

Internal Audit would like to thank all those who provided advice and assistance during the audit.

1. INTRODUCTION

1.1 Background

Public Safety Canada ("PS" or "Department") provides strategic policy advice and support to the Minister of Public Safety and Emergency Preparedness on a range of issues, including: national security, border strategies, countering crime and emergency management. The Department also delivers a number of grant and contribution programs related to emergency management, national security, and community safety, although these are generally related to providing resources to government organizations / jurisdictions or organizations and not specifically to individuals. The Department also coordinates the efforts of PS's Portfolio agencies as well as provides guidance on their strategic priorities.

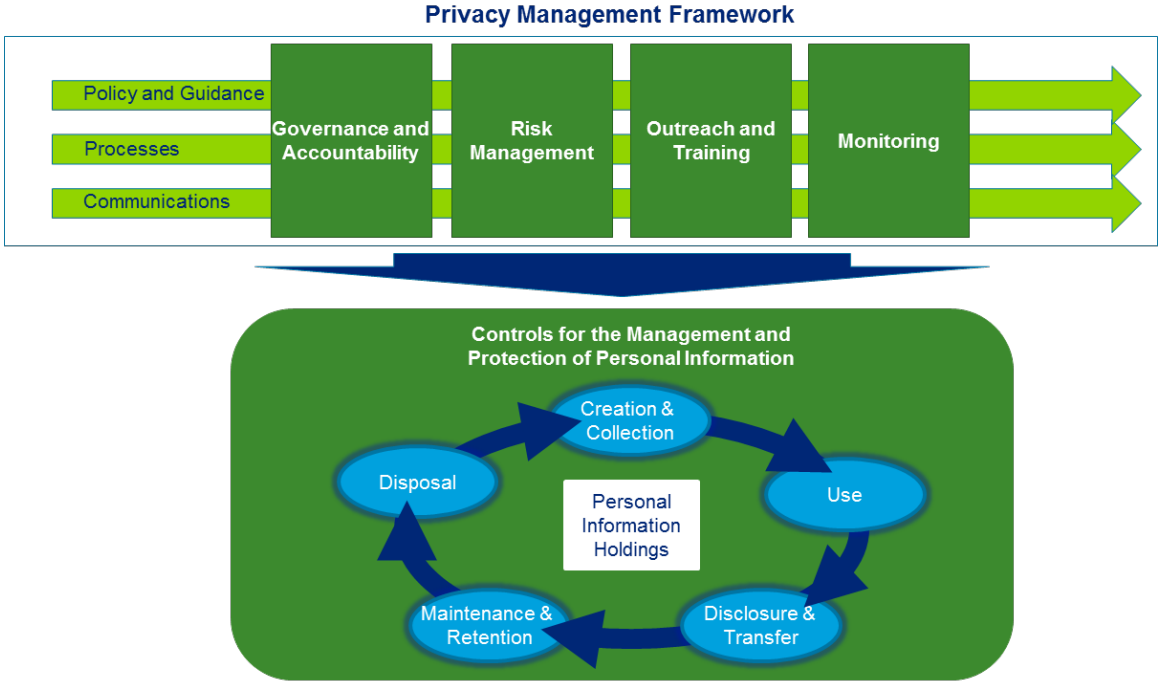
PS identified the management of personal information as an area that should be audited in 2014-15. Senior Management required assurance that the management control framework over personal information (i.e., Privacy Management Framework) was appropriately designed and operating effectively. Given the Department's role in policy coordination and advice, it does not collect a significant amount of personal information directly from the public, with only a small number of activities identified through the audit that collect and manage citizen-based personal information (refer to section 1.6 for additional information on these holdings). However, what it does manage is often sensitive in nature. The audit found that employee information represents one of, if not the largest, personal information holding.

The Office of the Privacy Commissioner of Canada (OPC) defines a Privacy Management Framework (PMF) as: *"… the way in which institutions organize themselves through structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and ensure compliance with the Privacy Act."* The purpose of the PMF is to build consensus around a set of privacy principles to guide the management of personal information in the Department. The PMF recognizes that new or unique privacy issues arise regularly and the Department cannot develop policies for every potential privacy issue, nor would such a massive suite of policies be desired or sustainable. Rather the PMF establishes a shared context for defining better privacy practices and for the identification and mitigation of potential privacy risks.

Although the elements required to support a PMF can be categorized in many different ways, for the purposes of this audit, they have been grouped into four main components:

- Governance and Accountability - Defining roles and responsibilities for privacy throughout the Department
- Risk Management - Assessing and managing privacy risk through the development and maintenance of appropriate guidance, as well as risk management processes such as Privacy Impact Assessments (PIAs) and Privacy Breach Management
- Outreach and Training - Ensuring staff and stakeholders understand their privacy rights and obligations through training and awareness activities, and maintaining relationships with external stakeholders such as the OPC
- Monitoring - Implementing monitoring and oversight mechanisms to ensure compliance with the Department's privacy obligations

Below is an illustrative example of the Privacy Management Framework described in the text above.



A privacy breach (i.e., unauthorized access to, or collection, use or disclosure of personal information) could have serious consequences for the reputation of PS, and may have operational impacts such as impeding the Department's ability to gain access to needed research data. Furthermore, given the Department's coordination and support role within the PS Portfolio, as well as outreach to other jurisdictions and stakeholders involved in public safety, any reputational harm may have serious impacts to the Government as a whole. Furthermore, a breach may result in departmental resources being required to investigate and respond to the breach, including addressing enquiries or audit activities from the OPC.

1.2 Legislative Framework

PS is subject to the *Privacy Act,* and must adhere to its requirements related to the management and safeguarding of personal information. The *Privacy Act* defines personal information broadly as "*information about an identifiable individual that is recorded in any form*". The *Privacy Act* protects the privacy of all Canadian citizens and permanent residents of Canada regarding personal information held by a government institution against unauthorized use and disclosure. The *Privacy Act* also gives Canadians, the right to access personal information held by the Government. Treasury Board Secretariat (TBS) has also implemented privacy-related policies and directives that provide additional requirements on the collection and management of personal information, including the *Policy on Privacy Protection*, *Directive on Privacy Impact Assessments*, and *Directive on Privacy Practices*.

1.3 Roles and Responsibilities

The *Privacy Act* outlines several powers, duties and functions given to the head of a government institution, for example those related to responding to privacy requests or disclosures under section 8(2) of the *Act*. The *Privacy Act* allows the head to "*designate one or more officers or employees of that institution to exercise or perform any of the powers, duties or functions of the head of the institution under this Act that are specified in the order*". While delegates are accountable for any decisions they make, ultimate responsibility still rests with the head of the government institution. PS has completed a Delegation Order per s. 73 of the *Privacy Act* outlining the roles and responsibilities that have been delegated to, among others, the Director Access to Information and Privacy (ATIP) and Executive Services and the ATIP Manager.

In addition to the administrative duties as outlined in the *Privacy Act*, the ATIP Division is responsible to ensure an appropriate PMF is established in the Department. The instruments required to be implemented by the ATIP Division to support the PMF components noted above include policy and guidance, processes such as the PIAs and Privacy Breach Management, and communications to staff and other internal and external stakeholders. Several of these policy, process and communication components are also required by the TBS, as outlined in the *Policy on Privacy Protection* and *Directive on Privacy Practices.*

The ATIP Division, situated within the Portfolio Affairs and Communications Branch, is comprised of 10 staff members, including the ATIP Manager, two Senior Advisors, five Analysts, a Junior Analyst and an Administrative Officer. Two positions have recently been staffed (September 2014) within the ATIP Division to form the Policy, Privacy and Training Unit.

In 2013-14, the ATIP Division received approximately 465 Access to Information requests and 68 Privacy requests. In addition to responding to requests made under the *Privacy Act* and the *Access to Information Act*, the ATIP Division provides the following services to the Department, as outlined in its *2013-14 Annual Report to Parliament on the Administration of the Privacy Acts*:

- Processing consultations received from other institutions;
- Providing advice and guidance to employees and senior officials on ATIP related matters;
- Producing the Annual Reports to Parliament;
- Delivering ATIP awareness sessions to departmental employees;
- Coordinating regular updates to Info Source manuals;
- Reviewing departmental documents, such as audits and evaluations, prior to proactively disclosing these on the departmental website;
- Developing departmental procedures for processing ATIP requests;
- Maintaining the Department's ATIP reading room; and
- Participating in forums for the ATIP community, such as the TBS's ATIP Community meetings and working groups.

Formally defined roles, responsibilities and accountabilities related to privacy outside of the ATIP Division are less formalized. The audit team was informed that this is due to ATIP Division resource constraints which have limited the development and implementation of privacy guidance and training within the Department. It should be noted that although the ATIP Division has the lead responsibility to provide the enabling policies, training and tools to ensure compliance with the *Privacy Act*, each employee is ultimately accountable to ensure the personal information in their custody and/or control is managed in accordance to the requirements of the *Privacy Act*.

1.4 Audit Objective

The objective of the audit was to provide reasonable assurance that the Department's Management Control Framework over the management of personal information is adequate and effective to ensure that the Department is in compliance with the *Privacy Act* and both TBS and PS related policies.

1.5 Scope

The scope of the audit, which covered the period ending April 30th 2015, included the examination of the accountability and policy framework as well as key procedures and other controls that are in place to:

- Ensure compliance to the *Privacy Act*, the TBS and PS associated policies;
- Define and communicate requirements in this area;
- Ensure an efficient and effective response to these requirements; and,
- Safeguard the Department's reputation and credibility as it relates to the Department's management of personal information.

The scope of the audit included both a review of the PS Privacy Management Framework as well as how the management framework has been applied to select personal information holdings collected and managed by PS. During the planning phase, personal information holdings across the department related to both PS employees and the public, in both electronic and hardcopy format, were determined, and based on these planning activities, those areas with personal information holdings selected for further examination during the conduct phase included:

- Emergency Management and Programs Branch (EMPB), which includes the **Programs Division** of the National Crime Prevention Centre. Through this division, PS provides funding related to the evaluation of third party initiatives meant to reduce crime.
- Community Safety and Countering Crime Branch (CSCCB), which includes the **Research Division** of the Research, Intergovernmental Affairs and Horizontal Policy Directorate. Through this division, PS conducts research related to community safety and crime, including the collection of personal information from other Canadian jurisdictions that wish to participate in the research.
- Community Safety and Countering Crime Branch (CSCCB), which includes the **Corrections and Criminal Justice Division** of the Corrections And Criminal Justice Directorate. Through this division, PS receives files from portfolio agencies for which PS performs

analysis in order to provide a recommendation to the Minister of Public Safety related to areas such as applications for the International Transfer of Offenders.

- National and Cyber Security Branch (NCSB), which includes the **Canadian Cyber Incident Response Centre (CCIRC),** that collects information on cyber security threats and incidents collected and managed.
- Corporate Management Branch (CMB), which includes the **Human Resources Directorate (HR)**, that collects and manages information related to employees.

The Personal Information processes within the Minister's office, were excluded from the scope of this audit.

For specific audit criteria refer to Annex A.

1.6 Risk Assessment

The risk assessment conducted in the planning phase of the audit informed the development of the audit scope and criteria. Identified potential risks were:

1. There is the risk of the lack of ATIP and business / functional area engagement throughout the Department, for example, ATIP involvement in the development of PIAs, Memorandums of Understanding (MOUs), and PIBs to ensure the consistent application of appropriate privacy practices and adherence to *Privacy Act* and TBS requirements.

2. There is a risk that a lack of policy and procedures, as well as appropriate training and awareness, for the management of personal information, could lead to the inappropriate or inconsistent management of personal information across the Department.

3. There is the risk of the collection of extraneous personal information not required by a Program area in order to fulfill their mandate.

4. There is the risk of excessive access to personal information that is retained in repositories such as RDIMS.

5. There is the risk of the inappropriate use or disclosure of personal information related to those files received by PS to perform analysis in order to provide a recommendation to the Minister.

6. There is the risk that employee information is not being appropriately used internally within the Department.

7. There is the risk of not having defined retention and disposal standards for personal information related to those files received by PS to perform analysis in order to provide a recommendation to the Minister, as well as personal information collected through cyber security activities.

1.7 Audit Opinion

PS has moderate issues related to the adequacy and effectiveness of the management control framework over personal information and compliance with the *Privacy Act* and TBS and PS related policies. There are opportunities for improving the management control framework over personal information to better identify risks and ensure appropriate monitoring to prevent and detect potential non-compliant activities.

1.8 Statement of Conformance and Assurance

The audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined

2. FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

Throughout the audit fieldwork, the audit team observed several examples of how controls are properly designed and applied effectively. This resulted in several observed strengths, examples of which are listed below:

- The department has ensured it has appropriate “incident management” practices in place in the event of a privacy breach. Specifically, the Department has developed and implemented privacy breach management policies and processes. The audit confirmed that privacy breaches brought to the attention of the ATIP Division were handled and followed-up on in an appropriate fashion.
- A policy and processes for the completion of Privacy Impact Assessments (PIAs) have been implemented, and those PIAs reviewed as part of the audit were completed and managed in an appropriate manner.
- The Department has defined delegation of authorities for the *Privacy Act*, and roles and responsibilities are clearly defined within the ATIP Division.
- Two positions have recently been staffed (September 2014) within the ATIP Division to focus on the further development and implementation of privacy policies and training.
- Through the sample access testing conducted during the audit, it was noted that access to personal information within PeopleSoft was well controlled. Furthermore, within the areas selected for the audit, access to hardcopy documents containing personal information was well controlled.
- Departmental employees encountered through this audit demonstrated an appreciation for the importance of safeguarding personal information.

The audit team also noted areas for improvement within the existing PMF and specifically for individual branch management practices and processes. These are outlined in the findings below.

2.1 Department Privacy Management Framework

The audit expected to find a comprehensive and effective PMF implemented within the Department, aligned with the requirements of the *Privacy Act* and PS and TBS policy requirements. While the current PS PMF is evolving and continues to mature, gaps were noted.

Governance and Accountability

The Department has defined appropriate delegation of authorities related to the *Privacy Act.* While roles and responsibilities within the ATIP Division have been clearly defined and communicated, job descriptions for some positions in the ATIP Division are out of date and need to be updated which is expected to be addressed through the Government of Canada (GC) ATIP Community Development Initiative Generic Work Description project.

Although roles and responsibilities for activities within the ATIP Division are clearly established, the privacy roles and responsibilities of the ATIP Division versus other functional areas in the Department were not as clearly defined or formally established. This has resulted in the ATIP Division not being consulted in a number of areas in which their input would have been appropriate. Furthermore, concerns were noted that program or functional areas may not recognize the ATIP Division as their first point of contact for privacy-related questions, and may instead consult with other groups (e.g., legal or security) within the Department or may seek advice directly from the OPC. Examples where roles and responsibilities require additional clarification and formalization include:

- Program areas did not appear to always be aware of the need to consult the ATIP Division on matters such as the privacy implications of agreements/contracts being put in place, or with respect to public interest disclosures (often consulting Legal Services instead of the ATIP Division). Given this, as an example, the ATIP Division does not have a departmental view of Memorandums of Understanding (MOU) that are in place between the Department and other entities. In addition, for the MOUs that are in place related to information sharing, they are not consistently developed and there was no formalized process for engaging the ATIP Division.
- Program areas do not always consult the ATIP Division regarding the development or inclusion of privacy language in contribution agreements. For example, the Department provides funding to third parties related to their crime prevention programs and research that takes place to evaluate the efficacy of these programs. The Department has limited the amount of personal information received through these contribution agreements to that of summary level results (without personal information). Despite this, the contribution agreements do not clearly define the privacy responsibilities of the recipients or the control and custody of the personal information.
- A privacy breach process has been implemented for the Department and audit testing revealed that those breaches reported to the ATIP Division were managed appropriately; however, program areas may not always report breaches to the ATIP Division in order to

consult with them to determine if there was a privacy breach. It should be noted that the departmental Privacy Breach Guidelines do require program officials to notify ATIP when a privacy breach occurs. Furthermore, there was no formalized process for sharing breach-related information from the Security Operations unit to the ATIP Division. Discussions with the Security Operations unit highlighted a number of breaches that may have included personal information that had not been reported to the ATIP Division.

Without clearly defined or formally established roles and responsibilities for privacy across all activities within the Department and greater clarity in regard to what constitutes personal information or a privacy breach, there is a risk that program areas do not understand the need to consult the ATIP Division, and appropriate privacy practices may not be carried out. Furthermore, this limits the ability of the ATIP Division to gain a full perspective on how personal information is collected and managed throughout the Department, making it difficult for the ATIP Division to identify and prioritize privacy risks and the actions required for mitigation. In addition, the lack of departmental policies and guidelines that specify privacy requirements for information sharing agreements increases the risk that privacy language is not included or consistent within the information sharing agreements, and may result in the parties to the agreement not understanding their roles and responsibilities related to privacy and the safeguarding of personal information.

Risk Management

For all five program areas that were selected for the audit, personal information being collected were appropriately managed, although for two of the five program areas, PIAs had not been conducted. Without completion of a PIA in program areas that manage personal information, there is a risk that personal information is not managed in compliance with the *Privacy Act*. At a minimum, program areas that collect personal information should document and retain a rationale for not having completed a PIA.

Although all the significant personal information holdings identified through the audit had a corresponding Personal Information Bank (PIB) entry in InfoSource, the audit noted some personal information holdings and their uses within those areas were not described through a PIB entry, specifically:

- Extradition requests to bring a Canadian offender who had left the country back to Canada were sent by CSC to the CSCCB for recommendation of ministerial approval; and,
- Royal Prerogative of Mercy requests to alleviate an individual from their sentence or modify the sentence were sent by the PBC to the CSCCB.

Without a formalized process for identifying the need for and appropriately updating PIB entries in InfoSource, there is a risk that all personal information holdings across the Department do not have a corresponding PIB registration in accordance with legislative requirements.

Outreach and Training

The ATIP Division noted that they have not been able to provide training sessions on the *Privacy Act* and departmental privacy processes due to resource constraints. A draft training plan had been developed which is expected to be implemented in 2015, with the short term training goals

to provide awareness sessions to senior management in the spring of 2015 and then rolling out training to the entire Department over the next three years.

The audit noted that the ATIP Division`s draft training plan could be improved through greater targeting of envisioned training to specific or higher risk program areas that collect and/or manage personal information in order to ensure employees handling personal information receive privacy training in a timely manner. A lack of training could result in employees not recognizing privacy issues, not understanding the need to consult the ATIP Division for matters that involve personal information, or not knowing what to do in the event of a privacy breach.

Monitoring

A process and corresponding metrics have not been established for the evaluation and measurement of the effectiveness of the implementation of the Department's PMF. Furthermore the regular monitoring of PI activities and breaches, while done, was not formalized. A lack of monitoring could result in the privacy program not being implemented appropriately or as intended.

Recommendations

1. The Assistant Deputy Minister Portfolio Affairs and Communications should develop and implement a formal plan, with defined timelines and accountabilities, to address the identified gaps in the Department's PMF. The plan should address:
   a. Defining roles and responsibilities related to privacy between functional areas as well as ensuring privacy considerations are embedded within business processes.
   b. Formalizing the process for updating PIB entries and reviewing PIBs so that all personal information holdings used for administrative purposes within the Department have a corresponding PIB entry in InfoSource. The ATIP Division should initially undertake a more comprehensive PIB update process to ensure an inventory of all personal information holdings is documented within the Department. This should also consider those personal information holdings used for non-administrative purposes.
   c. Establishing departmental policies and guidelines that specify privacy requirements for the development of information sharing agreements and contribution agreements.
   d. Revising and executing on the training plan to target training to specific or higher risk program areas that manage personal information, and implementing on a timely basis. The ATIP Division should coordinate their planned training with the baseline training offered by the Canada School of Public Service. As part of the training, it should be reiterated that program areas managing personal information should consult the ATIP Division and consider the need to complete a PIA. In addition, program areas that were identified as collecting and managing personal information without completing a PIA should either complete a PIA or document a rationale for not doing so.
   e. Establishing a monitoring program with related performance metrics for the evaluation and measurement of the privacy program's success, and presenting regularly to senior management (e.g. quarterly to the Departmental Management Committee) specifically on the status of key privacy matters.

#	Management Action Plan	Planned Completion Date
1	The Assistant Deputy Minister Portfolio Affairs and Communications will:	
	a. Reiterate that breaches involving personal information must be reported to the ATIP Office.	a. December 21, 2016
	Establish a departmental working group where Privacy can be integrated into business processes.	
	b. ATIP will require branches to identify all personal information holdings in their area of responsibility for both administrative and non-administrative purposes, confirm if a corresponding PIB exists, whether the PIB needs to be updated, and if none exists, complete a PIA to determine if one is required; and ensure that these updates/reviews happened as part of our normal business processes.	b. December 21, 2015
	c. Develop departmental policy tool/guidelines to assist employees in drafting Memorandum of Understanding / Information Sharing Agreements or Contribution Agreements when personal information is involved.	c. December 21, 2016
	d. ATIP to provide advice/training on how to complete PIAs and revise ATIP Training Plan to include focus on targeted areas in the department.	d. December 21, 2015 for targeted PIA training.
	e. Expand on the Weekly ATIP Lookahead to include performance metrics.	e. January 31, 2016
	Create a Privacy Community of Practice with the portfolio agencies to discuss common areas of concern and share best practices.	December 21, 2015.

2.2 Controls related to the Management of Personal Information

The audit expected to find that the Department is managing personal information holdings in compliance with the *Privacy Act* and applicable PS and TBS policies. The audit also expected to find that the Department appropriately collected, used and disclosed personal information in accordance with the *Privacy Act*, including having appropriate authority for collection, limiting collection to what was required for the identified purposes, and ensuring its use and disclosure were consistent with its original collection and limited to that which is necessary.

Although no major issues were noted with respect to how personal information was being collected, used, and disclosed in those areas that were tested within the scope of the audit, the processes related to how personal information is managed have not been formally documented. Without formally documented guidelines and processes for the management of personal

information, there is a risk that appropriate practices may not be followed, especially if there are changes in staff within the areas that manage personal information. Furthermore, formal standard operating procedures are critical to demonstrate to stakeholders and the OPC that appropriate processes have been established and are available to support the Department should a privacy breach occur. Specific observations related to the informal practices identified during the audit included:

- Human Resources has not formally documented their practices for responding to requests for reports and generating these reports; including outlining who should have access to these reports and the steps and considerations that should be taken to ensure the use of personal information is limited.
- CSCCB has not formally documented their processes through guidelines or standard operating procedures for managing personal information received from portfolio organizations for analysis and providing recommendations to the Minister (e.g. International Transfer of Offenders Act (ITOA[1]), disclosures of criminal records).

The Research Division within CSCCB conducts fairly extensive research with sensitive personal information. Specific operating procedures have not been formally established for research activities, although staff indicated that leading practices related to the management of personal information for research purposes were informally followed (i.e., Tri-Council Policy) . In addition, it was noted that there are no standard operating procedures or guidelines on privacy considerations, including entering into MOUs, collecting personal information, and matching or linking personal information for research purposes.

Additionally, program areas have very long or undefined retention periods for files containing personal information. Specific observations resulting from this audit include:

- CSCCB retains the files related to ITOAs and disclosures of criminal records for 10 years. This includes those files related to requests that have been withdrawn by the requestor (and therefore no decision made).
- The Research Division within CSCCB has generally not formally documented retention periods or disposed of any of personal information that is in its custody, and this includes extensive holdings of sensitive personal information related to offenders and criminal records, and research projects that have not been active for a number of years.
- CCIRC retains information indirectly received through the course of researching cyber incidents for 10 years, although Social Insurance Numbers (SIN) are immediately deleted, and financial information is deleted if it is identified.

Retaining personal information for longer than required increases the risk that the information may be inappropriately used or disclosed and may be considered a privacy breach. Furthermore, having longer retention periods than required increases the resource costs associated with managing the information.

Recommendations

[1] The International Transfer of Offenders Act (ITOA) enables offenders to apply to serve their foreign imposed sentence in their country of citizenship

2. Each Assistant Deputy Minister should formally document the processes for the collection, use and disclosure of personal information in those program areas that manage personal information. This should include clear guidelines related to the use of personal information so that there is a consistent understanding over what constitutes acceptable management and safeguarding of personal information.

3. Each Assistant Deputy Minister where applicable should review the retention periods for personal information to determine if the length of time is reasonable and ensure that these schedules are updated as required.

#	Management Action Plan	Planned Completion Date
2	Each Assistant Deputy Minister will, under the framework developed by ATIP,: - Develop/document processes for the collection, use and disclosure of personal information in personal information banks (P.I.B.); - Develop guidelines related to the use of personal information.	March 31, 2017
3	The Assistant Deputy Minister Corporate Management will: - Provide advice on identifying reasonable retention periods for records containing personal information. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch and ATIP, will: - Review/update the retention periods; - Develop a schedule for records containing personal information were retention periods do not exist.	March 31, 2017

2.3 Safeguarding of Personal Information

The audit expected to find appropriate security measures in place to ensure that personal information is appropriately protected and access is restricted. Based on the audit work conducted, the main repositories for files containing personal information within the Department are RDIMS, PeopleSoft, the network drive, and secure filing cabinets. While secure filing cabinets in the areas selected for audit and PeopleSoft access that was tested through this audit were well controlled, audit testing revealed weaknesses in access controls related to RDIMS and the network drive.

Files containing personal information saved in RDIMS are not always appropriately secured across the Department. Through audit sample testing, 10 of 25 documents containing personal information that were in RDIMS had excessive access permissions. Examples of excessive access includes individuals who were no longer on the team still having access to documents and access being inappropriately provided to all RDIMS users for some information. Hence, access

to documents is often granted on an individual basis to team members, rather than to user groups, increasing the likelihood of excessive access to documents because as employees leave or change jobs their ability to access historical files often remains unchanged. Additionally, when user group access is used, it may grant access to employees that should not be privy to the information.

Furthermore, monitoring by the Information Management Directorate found that there are approximately 10,000 files in RDIMS classified as Protected A or above that are not restricted. While the number has decreased in all Branches over the last year, there has been no formal follow-up on these documents as the Directorate's focus has been on ensuring Classified documents are being saved appropriately in the classified version of RDIMS rather than in the non-classified version of RDIMS.

The audit noted that within the Research Division within CSCCB, a large volume of sensitive personal information is being stored on network drives. Testing indicated that access was excessive, as a number of individuals within PS had access to a folder in which research information was stored without a need to have access to that information. Furthermore, a number of Shared Services Canada (SSC) employees had access to the folder given their role as system administrators, and files did not have further restrictions such as passwords or encryption. Excessive access results in individuals having access to personal information which is not required as part of their job duties and increases the risk of a privacy breach.

Recommendations

4. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch, where applicable should review the default access settings for documents in RDIMS that contain personal information. This should include the implementation of monitoring activities related to RDIMS access rights, and a process for follow-up and mitigation when excessive access rights are granted to documents containing personal information.

5. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch, where applicable should review any instances in which program areas are storing personal information on the Departmental network drives in order to:
    a. Determine if the use of the network drive for the storage of the personal information is appropriate;
    b. Review and ensure access is limited to only those individuals that have a requirement to access the information; and,
    c. Based on the sensitivity of the personal information, determine if additional controls should be implemented (e.g., file encryption) given that personal information stored on network drives may be accessible by network administrators, including network administrators with SSC.

#	Management Action Plan	Planned Completion Date
4	The Assistant Deputy Minister Portfolio Affairs and Communications will consistently advises that for documents of a personal nature, access should be strictly on a need to know basis. The Assistant Deputy Minister Corporate Management will: - Communicate RDIMS access control best practices and will ensure that best practices for access control are reflected in RDIMS training. - Develop a process for monitoring of documents above Protected A where excessive access rights have been granted. - Provide advice on corrective action to be taken when excessive access is granted to documents containing personal information. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch and ATIP, will: - Develop a protocol to address the accessibility of personal information in RDIMS, which will include a review of the use of default access settings.	March 31, 2017
5	The Assistant Deputy Minister Corporate Management will: - Provide advice on transferring this information into RDIMS; and, - Review the list of shared drive exceptions where program areas are still using network drives; - Develop recordkeeping agreements with each program area using a shared drive; and, - Establish a monitoring process to ensure appropriate use of shared drives. Each Assistant Deputy Minister, in collaboration with the Corporate Management Branch, will: - Review information on network drives, where applicable, and determine if they must be maintained on the shared drives; - Ensure that materials are properly relocated to RDIMS or Classified documents system as needed. Delete files off network and work with IT to permanently close them off; and, - Where applicable, review network policies to ensure	March 31, 2017

	appropriate use of files containing personal information.	

ANNEX A: AUDIT CRITERIA

Audit Criteria	Audit Sub-Criteria
Public Safety Canada has an effective Privacy Management Framework in place for the management of personal information that ensures compliance to the *Privacy Act*, the TB and PS associated policies	1.1 **Roles and Responsibilities** - Governance structure and roles and responsibilities for privacy are established, clearly defined, understood, and documented. 1.2 **Policies and Procedures -** Public Safety has policies, guides, manuals, protocols and processes for personal information management**.** 1.3 **Training, Awareness and Communication -** Appropriate training and awareness is provided to all staff, and is consistent with the privacy responsibilities of each position 1.4 **Monitoring and Reporting -** Mechanisms, including those addressing the assessment and mitigation of the risk of privacy breaches, are in place to effectively monitor and report on the management of personal information. 1.5 **Information Sharing Agreements / Third Parties –** Information sharing agreements involving personal information are appropriately documented, including roles and responsibilities related to the use and disposition of personal information.
Public Safety Canada is managing personal information holdings in compliance with the *Privacy Act* and applicable PS and TB policies.	**2.1 Collection -** Personal information is collected in accordance with *Privacy Act* requirements, including ensuring there is appropriate authority for collection, and collection is limited to that required for the identified purposes. **2.2 Safeguarding -** There are appropriate security measures in place to ensure that personal information is appropriately protected and access is restricted. **2.3 Use and Disclosure -**Personal information is used and disclosed in accordance with *Privacy Act* requirements, including ensuring its use and disclosure is consistent with its original collection and limited to that which is necessary. **2.4 Retention and Disposal -** There are mechanisms in place to ensure personal information is adequately retained and disposed of in accordance with approved retention and disposition schedules.