Gouvernement du Canada | Government of Canada

Canada

Respect ◆ Integrity ◆ Excellence ◆ Leadership

Serving GOVERNMENT, Serving CANADIANS.

Final review report

Review of Public Works and Government Services Canada's Privacy Management Framework

Public Works and Government Services Canada

Office of Audit and Evaluation

March 31, 2016

www.pwgsc-tpsgc.gc.ca

Table of contents

Introduction

1. This engagement was included in the Public Works and Government Services Canada (PWGSC) 2014-2018 Risk-Based Audit and Evaluation Plan.

Background

2. The *Department of Public Works and Government Services Act* establishes Public Works and Government Services Canada as a common service organization providing government departments, boards and agencies with support services for their programs. To deliver on its mandate, PWGSC collects, retains, and uses personal information in the administration of its services and programs.

3. The *Privacy Act* and *Privacy Regulations* provide the legal framework for the collection, retention, use and disclosure of personal information, and apply to federal government institutions. The *Act* also provides individuals (i.e. Canadian citizens and permanent residents) with a right of access to and correction of personal information about themselves that is under the control of a government institution.

4. Under the *Privacy Act*, personal information is defined as "information about an identifiable individual that is recorded in any form". Examples include information relating to an individual's name, address, race, education, national or ethnic origin, religion, age or marital status, criminal, financial or employment history, or a personal identification number (e.g. Social Insurance Number).

5. A privacy management framework is the way in which an institution organizes itself through structures, policies, systems, and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and meet its ongoing obligations under the *Privacy Act*. The *Policy on Privacy Protection* and *Directive on Privacy Practices* specify federal institutions' requirements with regards to sound management practices, including policies and protocols, clear responsibilities, privacy awareness, as well as monitoring compliance and public reporting. As per the *Policy on Privacy Protection*, "Heads of government institutions are responsible for the effective, well-coordinated, and proactive management of the *Privacy Act* and *Privacy Regulations* within their institutions."

6. Under Section 3 of the *Privacy Act*, the Minister of the department is designated as the head of the government institution for the purposes of the administration of the *Act*. Within PWGSC, the Assistant Deputy Minister – Policy, Planning and Communications Branch is the branch head responsible for privacy management. The Access to Information and Privacy (ATIP) Directorate (later referred in the report as Directorate), within the Policy, Planning and Communications Branch, administers the provisions of the *Privacy Act* for PWGSC, including the Translation Bureau, as well as the Office of the Procurement Ombudsman. The Directorate is accountable for developing and ensuring compliance with policies, procedures and guidelines, and for promoting awareness of the *Privacy Act.*

7. The Departmental Oversight Branch and Legal Services also have roles in the Department's privacy management.

    - The Departmental Oversight Branch, through the Director, Corporate Security and Associate Departmental Security Officer, is responsible for participating with the ATIP Coordinator (i.e. ATIP Director) in a cooperative process to ensure timely reporting, intervention and investigation into suspected or actual violations or breaches of security and/or privacy by departmental employees and persons engaged under contract for PWGSC.

- The Senior General Counsel's responsibilities include: providing legal interpretation and advice in relation the *Privacy Act*; advising the ATIP Directorate whether, in their opinion, the Cabinet exclusion provision is applicable, in the context of consultations on records that may be Cabinet confidences pursuant to section 70 of the *Privacy Act*; and, liaising between the ATIP Directorate and the Department of Justice's Litigation Office during judicial proceedings.

Privacy practices

8. Whereas the ATIP Directorate coordinates the management of PWGSC's privacy framework, controls over the collection, use and disclosure of personal information rest with branches and their program managers. Branches must therefore implement sound management practices in the handling of such information. The 2014 *Info Source*[1] chapter for PWGSC indicates that the Department has 26 Personal Information Banks[2]. Personal Information Banks are related to activities such as: pay and pension administration; document imaging services for Old Age Security and Canada Pension Plan; Receiver General's deposits and payments; controlled goods registry and industrial security clearances; supplier registration and integrity assessment program; seized property management program; and, shared travel services program. Business owners of Personal Information Banks are accountable for appropriate processing of personal information which includes collection, use, disclosure, safeguard, retention and disposal.

9. All employees have responsibilities under the *Privacy Act* for the management and handling of personal information. Thus, the *Departmental Policy on the Access to Information and Privacy Program (002)* applies to all departmental staff, including special operating agencies and the Office of the Procurement Ombudsman. Employees' responsibilities include: collecting, protecting, using, disclosing, retaining and disposing of personal information in accordance with sections 4 to 8 of the *Privacy Act*, the *Privacy Regulations* and the related TB policies and directives; promptly reporting any suspected or actual security breach involving personal information (i.e. privacy breach) to the Director, Corporate Security; promptly advising the ATIP Directorate of new or revised requirements to collect personal information, or use or disclosure personal information for a purpose for which it was not originally intended; and, providing the ATIP Directorate with complete, up-to-date and accurate descriptions of their organizations, programs and activities, as well as operational and personal information holdings under their control, for inclusion in the PWGSC chapter of *Info Source: Sources of Federal Government and Employee Information.*

Monitoring and reporting

10. The *Privacy Act* requires that federal institutions prepare an annual report to Parliament on the administration of the *Act*. Furthermore, heads of government institutions are required to identify, describe, and publicly report their Personal Information Banks in *Info Source.*

[1] *Info Source* is a series of publications containing information about the Government of Canada's access to information and privacy programs. The primary purpose of Info Source is to assist individuals in exercising their rights under the *Access to Information Act* and the *Privacy Act*.

[2] Info Source: Sources of federal Government and Employee Information 2014: http://www.tpsgc-pwgsc.gc.ca/aiprp-atip/ressources-resources/infosource2014-eng.html#a3.11

11. Non-compliance with the TB *Policy on Privacy Protection*, or its directives and standard may lead to various consequences. For example, the TB Secretariat of Canada will require non-compliant government institutions to provide additional information relating to the development and implementation of compliance strategies in their annual report to Parliament.

Focus of the review

Objective

12. The objective of the Review was to assess whether PWGSC has an effective privacy management framework, which includes: a governance structure; policies, procedures, and training; assessment of privacy impacts and risks; and investigation, reporting, and monitoring mechanisms, to help ensure compliance with Treasury Board and departmental policies and associated directives and requirements under the *Privacy Act*.

Scope

13. The scope of the planning and survey phase focused on the privacy management responsibilities of the ATIP Directorate (Policy, Planning and Communication Branch) and the Corporate Security Directorate (Departmental Oversight Branch) including how risks associated with the departmental privacy framework are being managed.

14. The Review of PWGSC's Privacy Management Framework did not examine the adequacy of the procedures in place to respond to requests under the *Privacy Act*. These procedures are similar to those being used to support the timely processing of access to information requests. The results of the planning and survey phase ranked this area as a low risk. The Review also excludes technologies supporting PWGSC's programs and services as the information technology's infrastructure is being provided by another government institution (i.e. Shared Services Canada) and some information management / information technology components were covered during previous internal and external audits (e.g. 2009-713 Audit of Classified Information Processed Electronically).

Statement of conformance

15. The Review conforms with the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program.

16. A review provides a moderate level of assurance by designing procedures so that the risk of an inappropriate conclusion being drawn based on the review procedures being performed is reduced to a moderate level. These procedures are normally limited to inquiry, analytical procedures and discussion. Such risk is reduced to a moderate level when the evidence obtained enables us to conclude that the subject matter is plausible in the circumstances.

Observations

17. The observations are intended to provide, based on the information gathered during the Review, a preliminary assessment of the existing situation against the Review objectives/scope as of September 30,

2015. This information, along with the risk assessment will be the primary source for the justification and rationale to not proceed with a comprehensive audit.

18. The risk assessment concluded that a comprehensive audit at this time would not add value to the Department. The Office of Audit and Evaluation was informed by the Director General Ministerial Services and Access to Information that PWGSC hired an external resource (consultant) to advise the Department on the implementation of the new *Anti-Terrorism Act, 2015* (also known as *Bill C-51*) and its privacy implications. The Director General noted that some of the findings contained in this report had been brought to her attention, particularly, those pertaining to governance and accountability. As part of her early observations, the consultant has recommended the creation of a Chief Privacy Officer position to oversee the administration of the *Privacy Act* at PWGSC. The Chief Privacy Officer position and a Director General level governance committee (i.e. Privacy Oversight Committee) have been established to support the management of privacy. As such, the work completed to date will add value to the Department without the need to complete a comprehensive audit.

19. Given the current work undertaken to date by the Office of Primary Interest to mitigate identified privacy risks, the Office of Audit and Evaluation will defer the conduct of a detailed engagement regarding PWGSC's Privacy Management Framework. A number of observations were identified during the Review that warrant the attention of management. The purpose of this Report is to formally communicate these findings to senior management to enhance the current PWGSC's privacy management framework.

Governance, accountability, roles and responsibilities

The Planning, Policy and Communications Branch is taking steps to strengthen the accountability and governance structures

20. To meet the obligations established under the *Privacy Act,* accountability for compliance with the *Act* must be well defined and communicated. Anticipating the impact of the new *Anti-Terrorism Act, 2015 (*also known as *Bill C-51)* on the privacy protection and the personal information management, PWGSC recently implemented a new governance structure to oversee the administration of the *Privacy Act.*

21. Established in June 2015, the Chief Privacy Officer position is held by the Director General for Ministerial Services and Access to Information of the Policy Planning and Communication Branch. The Chief Privacy Officer is responsible for the overall strategic direction and privacy compliance and has a mandate for departmental privacy oversight. The Chief Privacy Officer is accountable for the following:

    - overseeing and reviewing decisions related to information sharing agreements with other institutions made under the *Security of Canada Information Sharing Act*, privacy impact assessments and providing recommendations to the Deputy Minister
    - monitoring privacy threat risk assessments and resolution of privacy breaches, a shared responsibility with the Chief Information Officer and the Departmental Security Officer
    - liaising with the Office of the Privacy Commissioner on privacy-related matters; and
    - providing information, awareness, and training for the collection, use, disclosure, retention, and disposal of personal information; and, championing personal privacy rights to senior management

22. PWGSC also created a Privacy Oversight Committee to support the Chief Privacy Officer in overseeing the Department's compliance efforts while providing an overall strategic privacy direction and risk

management approach across the organization, although the Committee has not yet met. Chaired by the Chief Privacy Officer, the director general level committee will include representatives from the Accounting, Banking and Compensation Branch, the Departmental Oversight Branch, the Acquisitions Branch, the Chief Information Officer Branch and the Human Resources Branch.

23. The Chief Privacy Officer and the Privacy Oversight Committee will be supported by the Department's ATIP Coordinator who is responsible for providing technical and policy support to the Chief Privacy Officer. The ATIP Coordinator and staff within the Directorate also serve as the secretariat for the Privacy Oversight Committee. This Directorate is also responsible for establishing and directing all activities within the Department relating to the management of the departmental ATIP program, in accordance with the related PWGSC delegation instruments and the provisions of the acts, regulations, policies, directives, and guidelines.

24. Accountabilities under the *Privacy Act* have also been delegated through a delegation order (or instrument) pursuant the section 73 of the *Act.* Finally, roles and responsibilities of other Branches and other departmental staff in the administration of the *Privacy Act* are outlined in the departmental *Policy on the Access to Information and Privacy Program (002).*

25. Subsequent to the completion of our Review, we were informed several actions have been taken to advance these initiatives. A draft Terms of Reference outlining the Committee's mandate, membership, operations, and roles and responsibilities has recently been prepared. The draft Terms of Reference and the work plan of the new committee was expected to be presented to the Executive Committee on February 8, 2016 for approval. The Chief Privacy Officer is also required to report to the Executive Committee on his/her activities on an annual basis. The first report is expected to be presented to the Executive Committee in the 2016-17 fiscal year.

26. Further, the Directorate is considering a new organizational structure that would create two distinct but related programs (i.e. Access to information program and Privacy program). This new organizational structure will result in dedicated staff assigned to work on the departmental privacy program. Roles and responsibilities of staff assigned to work on privacy issues will include, but will not be limited to: processing privacy requests; developing privacy impact assessments; developing and maintaining information sharing agreements; and, conducting periodic privacy risk assessment.

Policies and procedures

Procedures and guidelines for the collection, use and disclosure of personal information are not formalized to ensure personal information is appropriately managed through its life-cycle

27. Policies, procedures and guidelines aid staff to effectively discharge their privacy responsibilities. Such policies and procedures must be available to employees, and structured with sufficient detail to facilitate an understanding of how an organization manages privacy. Organizations subject to the *Privacy Act* are responsible for developing and documenting internal policies that address obligations under the *Act*.

28. PWGSC has put in place its own policies for the management, administration and application of the *Privacy Act*. The departmental *Policy on the Access to Information and Privacy Program* outlines the Delegation of Authority and sets out the definitions, and the roles and responsibilities of all stakeholders within PWGSC. The Department has also implemented a suite of security and information management policies which contain privacy provisions. These include *Protection of Personal and Private Information*

in the Workplace, Records Management and Information Holdings, Forms Management Policy, Reporting of Actual and Suspected Breaches and Violations of Security, Departmental Security Program, and Policy on Information Management. The policies are available on the departmental Intranet site for the reference by all employees.

29. Departmental privacy policies do not, however, address some key aspects of the management of personal information such the collection, use, and disclosure of personal information, including the requirements for consent and notification. Furthermore, PWGSC has not formally established privacy protocols for the collection, use or disclosure of personal information for non-administrative purposes (i.e. the use of personal information for a purpose that is not related to any decision-making process that directly affects the individual, for example, for research and statistical purposes) as required by the TB *Policy on Privacy Protection*.

30. The Directorate has developed a number of directives and protocols to remedy the above noted gaps such as *Directive on Privacy Practices, Directive for the Non-Administrative Use of Personal Information,* and a *Protocol for the Non-Administrative Use of Personal Information*. These are intended to ensure that the collection, use or disclosure of personal information is carried out in compliance with the *Privacy Act*, TB policies and directives on privacy. To date, the directives and the associated protocol remain in draft.

31. The absence of overarching guidelines for the collection, use, and disclosure of personal information may lead to inconsistent approaches to personal information management across the Department. Enhancements of privacy policies, to address the above mentioned privacy issues, could bring a more uniform practice within PWGSC and ensure that personal information is appropriately managed.

Capacity, training and awareness

There is no formal privacy training provided to employees to provide them with the knowledge and awareness necessary to meet privacy obligations

32. A sound privacy management framework requires all members of an organization to be aware of, and ready to act on their privacy obligations. Training and awareness are important mechanisms to ensure compliance with the *Privacy Act* and achieving its objectives. Under the TB *Policy on Privacy Protection*, deputy heads or the delegates are responsible for ensuring that all employees are aware of their legal obligations under the *Privacy Act*, TB and departmental policies and procedures. At the present time, this responsibility resides with the ATIP Coordinator (i.e. Director, ATIP), although it will become the responsibility of the Chief Privacy Officer once the Officer position is fully implemented.

33. Privacy and security awareness training is provided to employees as part of PWGSC's On-Boarding and Orientation Program for new employees and the mandatory Security Awareness training for all public servants. Both the PWGSC-On-line Orientation Course (3959) of the On-Boarding and the Orientation Program and the On-line Security Awareness Course (A230) include a limited component on privacy and the handling of personal information. Program areas also provide to staff with personal information management responsibilities privacy training courses that are specific to their activities.

34. A number of privacy related initiatives have been undertaken to keep all departments employees up-to date on privacy matters. These include publications of two series of articles in "In The Know" entitled "ATIP and You", between February 2011 and May 2012. Two of the articles describe some features of

the *Privacy Act* and TB policies and directives on privacy protection. Awareness is also undertaken by the Corporate Security Directorate through articles in "In The Know", the Unit Security Officers Network (USON) and the security awareness week that is held annually at Headquarters and in the Regions.

35. Finally, the Directorate has been engaged in providing training and awareness sessions on both the Access to Information and Privacy (ATIP) Legislations and responsibilities to departmental managers and employees. For example, 15 sessions were given to 195 managers and employees at all levels from all branches of the Department during the fiscal year 2013-2014 according to the *Annual Report on the Privacy Act* on the administration of the *Privacy Act* . However, we identified through documentation review that the sessions were more focused on the process for access to information requests, rather than privacy and personal information management.

36. Despite the above, staff interviewed within the Directorate and the Corporate Security Directorate indicated that PWGSC lacks privacy training and a strong awareness program. There may be opportunities to enhance the Department's privacy training and awareness regime to help ensure compliance with the privacy obligations. Training employees helps ensure they have the required knowledge and skills to manage privacy in accordance with the *Privacy Act* and to fully comply with the Government of Canada and departmental privacy policies and requirements.

37. Subsequent to the completion of our Review, the Deputy Minister published a "From the DM's Desk" reminder to all staff regarding their role in protecting sensitive information in the workplace.

Risk assessment

Processes to manage risk associated with new or substantially modified programs or activities are not formalized

38. The TB *Directive on Privacy Impact Assessment (April 2010)* provides guidance to government institutions with respect to the administration of privacy impact assessment. The privacy impact assessment helps ensure that privacy implications are appropriately identified, assessed and resolved before a new or substantially modified program or activity involving personal information is implemented. To comply with the *Directive*, departments are expected to have in place mechanisms to identify and review new and substantially modified programs and activities that affect the management of personal information.

39. We determined that processes to assist program managers in evaluating the level of impact new or substantially modified programs and activities may have on individual's privacy and on managing the risks associated are yet to be formalized. PWGSC has developed a departmental *Directive on Privacy Impact Assessment* which is intended to provide employees with guidance on achieving their legal and policy responsibilities with respect to privacy for programs and activities involving the collection, creation, retention, use or disclosure of personal information. The Department has also developed a Privacy Protocol Assessment template. The purpose of the template is to assist staff in identifying any potential privacy risks associated with personal information that is used by PWGSC for a non-administrative purpose and provides strategies to mitigate privacy risks that may be identified. However, to date, the *Directive on Privacy Impact Assessment* and the Privacy Protocol Assessment template are still in draft form.

40. Though there are no formal processes in place for privacy impact assessment development and approval, the Directorate management indicated that a privacy impact assessment is undertaken when it is deemed necessary. Program areas usually consult with the Directorate for guidance when proposing new programs and activities or substantially modifying an existing one to determine whether a privacy impact assessment is required. The Directorate will recommend during this consultative exercise the development of a privacy impact assessment when necessary. However, there are issues with the application of this process as it is time consuming, burdensome and inefficient.

41. Although privacy impact assessment may be undertaken when deemed necessary, there is a need to establish a formal process that results in more timely assessments, with responsibilities and accountabilities fully defined to evaluate potential privacy risks when new programs, or activities, is implemented, in accordance with the TB *Directive on Privacy Impact Assessment*. Until this is implemented, privacy impact assessment processes may vary across branches, and there remains the possibility that privacy risks will go undetected and hence unmitigated.

42. Subsequent to the completion of our Review, we were informed the Directorate will be more involved developing privacy impact assessments. The Directorate indicated that they would take on the responsibility of leading the writing privacy impact assessment in collaboration with the program areas. Program areas will validate information included in the draft document prior to its approval. In addition, the Privacy Oversight Committee (i.e. the Chief Privacy Officer) intends to develop a plan that identifies risks to privacy associated with the Department's new activities and programs. The Chair of the Committee (i.e. Chief Privacy Officer) has requested members to establish a list of all initiatives and programs that will need a privacy impact assessment completed in the coming year. The list will serve to create a master table, which will serve as basis of the Committee's work in identifying risks to privacy associated with new or substantially modified programs or activities.

Processes for managing personal information shared with third parties are not in place.

43. Under the Privacy Act, institutions that are transferring to or sharing personal information with a third party for processing remain responsible for the personal information. The Act and related TB policies and directives require departments to: develop arrangements or agreements regarding the exchange of such information; define the extent of the sharing; and, identify the controls that are in place to protect personal information.

44. PWGSC shares personal information with government security institutions and law enforcement bodies for the purposes of issuing employment security clearance, national security investigations and other investigative functions described under paragraph 8(2)(e) of the Privacy Act.

45. We found limited evidence of procedures in place to ensure that information exchanged with third parties is protected and handled in accordance with the requirements of the *Privacy Act*. Information gathered through document review indicates that while there are some Information Sharing Agreements in place, the Department does not maintain an inventory of its information sharing agreements nor does it undertake a periodic review for updating such agreements. Furthermore, though security clauses are routinely included in contracts, it is not clear whether they contain necessary privacy clauses.

46. For personal information shared with contractors and services providers, the Department, through its Integrity Programs and Services/Contract Security Program, has established mechanisms to safeguard Canadian and foreign government's sensitive information and assets entrusted to private-sector companies that are under government contract. The mechanisms include: evaluating, assessing risk and

granting security clearance to the companies and their employees; conducting security inspections of companies; and, negotiating and administering international bilateral industrial security arrangement.

47. Having mechanisms in place for managing personal information shared with third parties (i.e. contractors/services providers, other government institutions) could help ensure that information disclosed or used by third parties is handled according to sound privacy practices. Lack of controls over personal information exchanged with third parties may lead to: inconsistent practices throughout the Department with respect to personal information sharing; non-compliance with privacy obligations when the organizations' functions or services are performed under contract by third parties or when disclosing personal information to other government institutions; and, non-compliance with notification and reporting requirements respectively to the Privacy Commissioner and Parliament in that regard.

48. The TB Secretariat developed, in collaboration with the Institute for Citizen-Centred Service, best practices guidelines for *Government-to-Government Personal Information Sharing*, which provides useful advice and strategies to minimize privacy risks within personal information sharing agreements. The guidelines offer templates to assist government institutions in their work on such agreements. TB Secretariat also issued other guidance that would apply to contracts and service agreements with third parties involving personal information entitled: *Taking Privacy into Account Before Making Contracting Decisions*. These guidelines are valuable and applicable with respect to information sharing practices and could be used by PWGSC in establishing controls over personal information handled by third parties.

49. We did not examine PWGSC's personal information sharing practices in detail at this phase of the Review. Other branches/sectors within the Department exchange information in the course of administering programs such as the federal pensions' administration, public service employee and benefit plans, controlled goods program. In those instances, personal information may be shared with governments' institutions for verification of pension coverage (e.g. Employment and Social Development Canada, Department of National Defense, Royal Canada Mounted Police) or with private sector insurance plan administrators for benefit purposes (e.g. Sun Life, Great-West Life). Additional evidence will be gathered during the planned Audit of PWGSC Privacy Practices to confirm measures in place to help ensure that the Department continues to fulfill its privacy obligations under the *Act* when contracting out a program or service delivery function to third parties.

Monitoring and reporting

Mechanisms for reporting and investigating privacy breaches are in place

50. According to the TB *Guidelines for Privacy Breaches*, "A privacy breach involves improper or unauthorized collection, use, disclosure, retention or disposal of personal information. A breach may occur within an institution or off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders." Under the TB *Directive on Privacy Practices*, government institutions are responsible for implementing a plan for addressing privacy breaches should they occur.

51. In accordance with TB *Directive on Privacy Practices*, PWGSC established, in June, 2015, a *Privacy Breach Protocol* for addressing privacy breaches. The purpose of the protocol is to help the Department respond to incidents of improper or unauthorized access to or disclosure of personal information in an effective and coordinated manner. The Department has adopted a collaborative approach, with staff from the Directorate and the Corporate Security Directorate working together, to investigating privacy breaches. Other corporate stakeholders (e.g. Communications Sector and the Information Technology

Security Compliance Directorate) may be involved as needed. Procedures and tools for responding to a privacy breach are outlined and provided in the *PWGSC Privacy Breach Protocol*. We reviewed the protocol and determined that it complies with the breach reporting recommendations established by the TB Secretariat. Specifically, the protocol defines roles and responsibilities should a breach occur and provide guidance for an effective resolution, including the following key steps: (1) discovery and reporting; (2) full assessment; (3) notification; (4) mitigation and remediation.

52. Departmental Oversight Branch (i.e. Corporate Security Directorate and Industrial Security Sector) has also developed internal procedures to ensure that in the case of a security incident related to personal information, employees involved are aware of their roles and responsibilities and can minimize the impact of unauthorized access to personal and protected information or assets. The procedures (i.e. *(i) Privacy Breach Investigation Standard Operating Procedures; and (ii) Handling of Security Incident Involving Misdirected Personal Information)* are based on the PWGSC *Privacy Breach Protocol* and provide information on what must be done when a privacy breach occurs and how to prevent privacy breaches.

53. The Corporate Security Directorate also establishes performance indicators for investigating security breaches that could lead to privacy breach. Investigation into an actual or suspected privacy breach must be completed and closed within 90 calendar days of the incident being reported to the Security Investigations Unit of the Directorate. The Review team learned that the Directorate is having challenges investigating privacy breaches. As a result of improved employees' awareness, the number of alleged breaches reported has increased over the past year, and they are not able to meet their 90 days' timeframe. Though in the past, the Directorate exceeded the target (85%) with a rate of 90-95% completed within the 90 day deadline, investigators are now able to complete only 70% of their investigations within 90 days. Given these circumstances, the Directorate indicated that breaches will be investigated in the future on a case by case basis, with priority given to material breaches.

54. While privacy breaches are investigated, it is not clear whether corrective measures are implemented to reduce risk of reoccurrence. Without monitoring to ensure that corrective measures are implemented, there is a risk that breaches may reoccur. The Review did not look into practices in program areas and as such we could not confirm whether recommendations stemming for breach investigation are implemented. The planned Audit of Privacy Practices will examine corrective measures undertaken by program areas following an investigation.

55. Statistics provided by the Departmental Security Officer and the ATIP Coordinator show that between April 1, 2013 and November 30, 2015, there were 151 alleged (suspected) privacy breaches reported to the Departmental Security Officer, of which 123 were founded (See Table 1 for details).

Table 1: Number of Alleged and Actual Privacy Breaches per Year

Year	Alleged	Actual
2013-2014	**19**	**12**
2014-2015	**36**	**24**
2015-2016[(1)]	**96**	**87**
Total	**151**	**123**

[(1)] The numbers are based on the period from April 1 to November 30, 2015 (this is the period to consider whenever reference is made to statistics on privacy breaches during the fiscal year 2015-2016 in the Report)

56. Administrative errors comprise 90% of all actual privacy breaches from April 1, 2013 to November 30, 2015. Other privacy breaches include lost, disclosure, protection and stolen categories. Table 2 provides a breakdown of the categories of privacy breaches. Appendix A provides privacy breach category definitions.

Table 2: Actual Privacy Breaches by Category

Category	2013-2014	2014-2015	2015-2016	Total	Percentage (%)
Access					
Administrative Error	10	20	81	111	90
Collection					
Disclosure	1	1	4	6	5
Lost	1	1	1	3	2
Protection		1	1	2	2
Stolen		1		1	1
Use					
Other: Cyber-attacks					
Total	**12**	**24**	**87**	**123**	**100**

57. The number of actual privacy breaches by branch from April 1, 2013 to November 30, 2015 appears in Table 3. The two branches with the largest number of breaches are Accounting, Banking, and Compensation Branch and Departmental Oversight Branch. This may be due to the fact that they process a large volume of personal information given the nature of their activities and programs.

Table 3: Number of Actual Privacy Breaches by Branch in the National Capital Region (April 1, 2013 to November 30, 2015)

Branch	2013-2014	2014-2015	2015-2016	Total	Percentage (%)
Accounting, Banking and Compensation	8	20	32	**60**	**49**
Acquisitions					
Chief Information Officer					
Departmental Oversight	1	1	48	**50**	**41**
Finance and Administration					
Human Resources		1	2	**3**	**3**
Integrated Services		1	1	**2**	**2**
Legal Services					
Parliamentary Precinct	1			**1**	**1**
Policy, Planning, and Communications	1		4	**5**	**4**
Real Property					
Translation Bureau					
Total	**11**	**23**	**87**	**121**	**100**

While Public Works and Government Services Canada's meets Treasury Board Secretariat mandatory reporting requirements on the administration of the *Privacy Act*, the Department could benefit from ongoing monitoring to ensure that applicable policies and procedures are consistently adhered to across the organization

58. Monitoring and reporting allows organizations, subject to the *Privacy Act*, to assess whether they are meeting policy and directive requirements in place to support appropriate administration of the *Act*. They also ensure that senior management is informed, on a regular basis as to whether the privacy management framework is functioning as expected. Heads or their delegates are responsible for monitoring compliance with the TB *Policy on Privacy Protection* as it relates to the administration of the *Privacy Act*. Further, departments are to report annually on their administration of the *Act* as required by section 72 of the *Act*.

59. In accordance with the requirements of the *Policy on Privacy Protection*, PWGSC prepares and tables in Parliament an annual report on the administration of the *Act*. The most recent available report (i.e. *2013-2014 Annual Report on the Privacy Act*) provides information such as the number of material privacy breaches reported to the ATIP Directorate or the Corporate Security Directorate, multi-year statistics, with interpretation and explanation of trends, on requests made under the *Act*. The Report also outlines privacy impact assessments completed and new or revised Personal Information Banks registered during the fiscal year. The report does not, however, contain information on day-to-day monitoring, privacy issues identified during the year, or risks associated with the Department's activities and how it responds to them.

60. The Assistant Deputy Minister, Policy, Planning and Communications Branch, who is the branch head responsible for privacy, also used management level committees (i.e. Executive Committee) to inform senior management of privacy matters within PWGSC. The presentations addressed privacy risks and proposed actions to reinforce the Department's privacy management framework.

61. While consideration of privacy-related issues at management level committees ensures that management has a mechanism for ongoing monitoring of privacy concerns, there is no indication that the committees' review or follow-up on corrective actions taken to address privacy concerns. For example, the presentation to the Executive Committee of February 13, 2013 entitled "*Privacy Framework for PWGSC – Areas of Risks*" outlined privacy risks within the Department and proposed actions to reinforce the organization's privacy management framework. Following the presentation, the Deputy Minister requested that Branch and Regional management teams assess regularly their vulnerability in terms of sensitive records, accessibility and transmission/manipulation of data, and actions related to information management. During the February 13, 2013 presentation, the Assistant Deputy Minister responsible for privacy proposed, as action to reinforce PWGSC's privacy management framework, to develop a management action plan and report on its implementation to the committee within 12 months. However, no corrective actions were undertaken to address privacy risk and gaps as expected; the Directorate indicated that it was later decided that issues identified in the presentation to the Executive Committee were not of major concern to the Department, and as such a management action plan was not necessary. We were however unable to obtain any evidence pertaining to this decision.

62. The *Annual Report on the Privacy Act* is the only formal monitoring and reporting tool used to assess and report on the management and administration of the *Privacy Act* within PWGSC. We believe there are opportunities to strengthen monitoring mechanisms. For that purpose, the Department could assess whether its current monitoring mechanisms are appropriate for the size and complexity of its mandate and the risks associated with the personal information administered.

Conclusions

63. Overall, the Review showed that while certain elements of a comprehensive privacy management framework are being put in place, there remains gaps/opportunities for improvement in relation to the framework to help ensure compliance with TB and departmental policies and associated directives and requirements under the *Privacy Act*.

64. A new governance structure, with the appointment of a Chief Privacy Officer and the creation of Privacy Oversight Committee, has been created to provide a coordinated and consistent approach to managing privacy across the organization. PWGSC has developed a *PWGSC Privacy Breach Protocol* for responding to incidents of improper or unauthorized access to or disclosure of personal information in an effective and coordinated manner.

65. There are, however, important gaps that need to be addressed and opportunities where PWGSC could strengthen its privacy management framework to ensure that the Department meets its privacy obligations under the *Privacy Act* and related TB and departmental policies. These include:

    - implementing overarching procedures and guidelines for the collection, use and disclosure of personal information to ensure the information is appropriately managed
    - enhancing privacy knowledge and awareness, including training specifically tailored to employees' duties/roles
    - formalizing privacy risk management processes to ensure that potential privacy risks associated with new programs or activities are identified, monitored, and mitigated
    - establishing mechanisms for sharing personal information with third parties to ensure compliance with relevant privacy obligations under the *Privacy Act*; and
    - assessing whether current monitoring mechanisms are appropriate for the size and complexity of the Department's mandate and the risks associated with the personal information administered

66. We did not examine privacy practices across the Department, nor attempt to prescribe every element of a privacy management framework. Subsequent to the completion of our Review, the Directorate provided additional information on action being undertaken to address identified gaps and enhance the Department's privacy management framework, specifically in the areas of governance, privacy risk management and breach management. A comprehensive audit would have allowed for the gathering of additional evidence to confirm whether PWGSC has an effective privacy management framework to ensure compliance with TB and departmental policies and associated directives and requirements under the *Privacy Act*. However, given the current work being undertaken by the Office of Primary Interest to mitigate identified risks, the Office of Audit and Evaluation will defer the engagement. Consideration of the re-launch of an audit at a future date will be part of the Office of Audit and Evaluation's annual planning process. This report outlines our observations to be considered by the Department in its effort to build an effective privacy management program. The Office of Audit and Evaluation will examine privacy practices in detail within branches/program areas during its planned Audit of PWGSC Privacy Practices to confirm controls in place to help ensure that staff comply with their obligations under the *Privacy Act*.

Recommendation

It is recommended that the Assistant Deputy Minister, Policy, Planning and Communications, should consider the gaps identified in the development of their action plan to enhance the Privacy Management Framework.

Management response

We have had the opportunity to review the Chief Audit and Evaluation's Report of 2014-710 Review of PWGSC's Privacy Management Framework and agree with the conclusions and recommendations found therein. The Review Report is timely as we are in the midst of transforming our privacy program to ensure better support to senior management as well as a more proactive approach to managing privacy-related risk in the Department. Highlights of actions taken to date include the creation of a Chief Privacy Officer, establishment of a robust governance structure, and revisions to the process for Privacy Impact Assessments. As we continue our transformation efforts, the results of the Review Report provides valuable guidance to ensure that we are establishing a robust privacy program. Planned actions are identified in our detailed Management Action Plan.

Management Action Plan

The Assistant Deputy Minister, Policy, Planning and Communications will:

1.1 Implement the privacy management governance structure, including defining and communicating roles and responsibilities for privacy management.
- 1.1.1 Implement Chief Privacy Officer function and Privacy Oversight Committee.
- 1.1.2 Develop a Privacy Impact Assessment Environmental Scan.

1.2 Publish the Privacy Breach Protocol on the departmental intranet site and communicate it to PWGSC employees via *In The Know.* Access to Information and Privacy (ATIP) Directorate and Corporate Security Directorate have already implemented the protocol.

The protocol provides the roles and responsibilities of departmental stakeholders should a breach occur, and step by step procedures for responding to a privacy breach, including discovery and reporting, assessment, notification, mitigation and remediation.

1.3 Submit the new Directive on Privacy Practices to the Departmental Policy Unit to proceed with the approval process in accordance with the Framework for departmental policy instruments within PWGSC (003).

The new directive defines the roles and responsibilities of all stakeholders with respect to privacy management in the Department, including the development of privacy impact assessments for new or substantially modified programs or activities and monitoring related actions plans, information sharing with third parties, etc.

1.4 Finalize the draft Privacy Protocol for Non-Administrative Uses of personal information and submit it to the Privacy Oversight Committee members for review and comments, and then to the departmental Chief Privacy Officer for approval.

1.5 Prepare a communications plan, in consultation with the Communications Sector, to make PWGSC employees aware of the new privacy policy instruments.

1.6 Develop and initiate implementation of a privacy risk-based and targeted training program to raise PWGSC employee awareness of privacy obligations under the *Privacy Act* and related policies.

1.7 Update the list of ongoing and anticipated Privacy Impact Assessments (PIAs) to serve as the basis for identifying risks to privacy associated with new or substantially modified programs and activities.

1.8 Report annually to EXCO on the state of privacy in the Department and take these opportunities to assess the efficiency of our program, governance and policy framework as well as our monitoring mechanisms.

We will use a variety of factors to determine the areas more at risk, such as number of Personal Information Banks, personal information systems, privacy breaches, frequency of sharing of information, etc. We will measure outputs such as number of sessions, number of employees "trained", distribution of awareness material as well as outcomes (for example, decrease/increase in the number of privacy breaches).

About the Review

Authority

This engagement was included in the Public Works and Government Services Canada (PWGSC) 2014-2018 Risk-Based Audit and Evaluation Plan.

Objective

The objective of the Review was to assess whether PWGSC has an effective privacy management framework, which includes: a governance structure; policies, procedures, and training; assessment of privacy impacts and risks; and investigation, reporting, and monitoring mechanisms, to help ensure compliance with Treasury Board and departmental policies and associated directives and requirements under the *Privacy Act*.

Scope and approach

The scope of the planning and survey phase focused on the privacy management responsibilities of the ATIP Directorate (Policy, Planning and Communication Branch) and the Corporate Security Directorate (Departmental Oversight Branch) including how risks associated with the departmental privacy framework are being managed.

The Review of PWGSC's Privacy Management Framework did not examine the adequacy of the procedures in place to respond to requests under the *Privacy Act*. These procedures are similar to those being used to support the timely processing of access to information requests. The results of the planning and survey phase ranked this area as a low risk. The Review also excludes technologies supporting PWGSC's programs and services as the information technology's infrastructure is being provided by another government institution (i.e. Shared Services Canada) and some information management / information technology components were covered during previous internal and external audits (e.g. 2009-713 Audit of Classified Information Processed Electronically).

The Review was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

The Review was conducted to gain an understanding of the subject area by reviewing and analyzing relevant departmental/branch/sector policies, processes and documentation provided by the ATIP Directorate, the Corporate Security Directorate, and the Information Technology Security Directorate within the Chief Information Officer Branch. Information was also gathered through interviews with key directors, managers, and staff within the Policy, Planning and Communication Branch, the Departmental Oversight Branch, and the Chief Information Branch.

Criteria

The Review criteria were developed after conducting a risk assessment, and are based on the requirements of the *Privacy Act*, the TB *Policy on Privacy Protection* and its related directives and guidelines governing the management of personal information and the departmental *Policy on the Access to Information and Privacy (ATIP) Program (DP02)*.

The criteria are as follows:

- PWGSC has a privacy management framework in place that includes governance, policies and procedures as well as an effective training and awareness program to support the effective management of personal information.

- Privacy risks associated with new or significantly modified systems, programs and activities that involved the use of personal information are identified and mitigated.

- Privacy breach investigation, reporting and resolution mechanisms are developed and implemented. Procedures are established to ensure that employees and third parties that cause privacy breaches are informed of privacy policies/protocols and consequences for not complying with such policies.

- Procedures and controls are established to ensure compliance with the *Privacy Act* when sharing personal information with third parties (i.e. private sector organizations, federal government institutions, and other public sector organizations).

- Procedures are in place to ensure consistent monitoring and reporting on the administration of the *Privacy Act*, including a process to address privacy related complaints and disputes.

Review Work Completed

Review fieldwork for this review was substantially completed on September 30th, 2015

Review Team

The Review was conducted by members of the Office of Audit and Evaluation, overseen by the Director of Internal Audit and under the overall direction of the Chief Audit and Evaluation Executive.

The Review was reviewed by the quality assessment function of the Office of Audit and Evaluation.

Appendix A: breach category definitions[3]

1. **(Access) Inappropriate access to personal information:** Where an employee has accessed personal information stored in paper records or on a government information system.

2. **Administrative Error:** This category includes incidents that are minor in nature and involve errors as a result of the inappropriate handling of government correspondence (e.g. email, mail, faxes, and physical documents that are inadvertently issued to an inappropriate recipient), and telephone transactions involving improper steps to identify a client. When an incident is coded into this category it is also to be assigned to one of the following sub-categories:

    a. **Account error:** Where a program area inadvertently updates the wrong account holder's information (*i.e.*, to add a dependent to an account, to change an address, etc.), but the error is discovered without any correspondence (in any form) being issued.
    b. **Bad Address:** Includes incidents where an individual moves, but does not update their address held by government, which results in correspondence being issued to the incorrect location.
    c. **Email:** Where an email containing personal information is sent to an unauthorized person. This includes government employees receiving emails intended for another government employee who has a very similar name.
    d. **Fax:** Where a fax containing personal information is sent to an unauthorized person.
    e. **In-person:** Where personal information is physically handed to an unauthorized person during a client interaction. This includes cheques and other documents being issued to the incorrect individual.
    f. **Mail:** Where paper-based correspondence sent by traditional mail or courier is sent to, or received by, an unauthorized person. This includes "double-stuffed" envelopes, lost mail, and other incidents where mail is the mechanism by which the records are transited.
    g. **Other:** Administrative/processing errors that do not fit into one of the other sub-categories.
    h. **Telephone:** Administrative errors related to improper identification or verification of a client.

3. **(Collection) Inappropriate collection of personal information:** Where government inappropriately collects personal information from an individual (e.g. without consent or without a proper collection authority).

4. **(Disclosure) Inappropriate disclosure of personal information:** Includes verbal and other disclosures (e.g. improperly unredacted files related to a court proceeding) of personal information to individuals not authorized to receive it.

5. **Lost:** Incidents involving a loss of government records containing personal information. This includes losses of paper records and electronic records stored on a technology device (cellular telephone, computer, thumb drive or other portable storage device) that was unencrypted (e.g. personal device) and/or insecure (e.g. password taped to side).

6. **(Protection) Inadequate protection of personal information:** Incidents where there has been no apparent disclosure or exchange of personal information, but there is a situation where a public body has not ensured that reasonable security measures are in place to protect personal information.

[3] Source: Privacy Investigation Unit of the Office of the Information & Privacy Commissioner for British Columbia

7. **(Stolen) Stolen asset - includes paper records:** Incidents involving a theft of government records containing personal information. This includes thefts of paper records and electronic records stored on a technology device (cellular telephone, computer, thumb drive or other portable storage device) that was unencrypted (e.g. personal device) and/or insecure (e.g. password taped to side).

8. **(Use) Inappropriate use of personal information:** Where a government employee or unit makes an improper use of personal or business sensitive information.

9. **Other - Cyber-attacks:** Cyber-attack of data systems through malicious code (e.g. automated virus), hacking or phishing which result in a breach of personal information. These incidents are typically waged by non-government actors.