Public Works and Government Services Canada
Audit Services Canada

Travaux publics et Services gouvernementaux Canada
Services de vérification Canada

Assessment of Veterans Affairs Canada's Compliance with the *Access to Information Act* and *Privacy Act*

Date: July 2011

Prepared by:

Audit Services Canada from

Public Works and Government Services Canada

ASC SVC
Canada

Table of Contents

Executive Summary

The *Access to Information Act* gives Canadian citizens, permanent residents, or any person or corporation present in Canada a right to access information that is contained in government records. The *Privacy Act* provides them with the right to access their personal information held by the government, and protection of that information against unauthorized use and disclosure.

In October 2010, the Office of the Privacy Commissioner released a report in response to a complaint alleging Veterans Affairs Canada's mishandling of a Veteran's personal information. The Privacy Commissioner concluded that the Department was not compliant with federal privacy legislation and lacked the controls to protect sensitive information from being widely disseminated within the Department. In response to these findings, the Department prepared a 10-point action plan outlining the corrective measures that would be taken.

We were engaged to complete step nine of the action plan – an independent assessment of the Department's compliance with the *Access to Information Act* and the *Privacy Act*. Our assessment criteria were drawn from the sections of the Acts for which the Department has responsibility. Management agreed with the suitability of these criteria. At the Department's request, our scope was expanded to assess its progress in implementing the 10-point action plan.

This was an assessment, not an audit, and was therefore not designed or performed to provide a high level of assurance. Our assessment approach consisted of inquiry and review of documentation to gather evidence of the Department's compliance with the Acts. Our findings apply to the period when we conducted our assessment, April 1 to May 31, 2011.

The Department has worked to reduce the risk of a future privacy breach introducing policies and procedures to prevent and detect the misuse of clients' personal information by its employees. Given the recent implementation of these changes, we could not assess the effectiveness of the policies and procedures in achieving compliance with the Acts. Employee education and training are now critical to successful implementation of the new policies and procedures.

The Acts require the Department to respond to requests for information within 30 days. We found that in 2010-11 the Department completed roughly 70 percent of requests within the legislated time frame. With respect to the disposal of personal information in accordance with established records retention periods, we found that the Department was not disposing of electronic records maintained in its Client Services Delivery Network system.

At May 31, 2011, the Department had substantively completed its 10-point action plan. Five of the 10 steps were completed and 5 were ongoing; employee training and monitoring are continuing. The Department plans to complete all actions prior to the Privacy Commissioner's audit, anticipated in fall 2011.

This report contains four recommendations for improvement to which management has agreed.

Introduction

The *Access to Information Act* gives Canadian citizens, permanent residents, or any person or corporation present in Canada a right to access information that is contained in government records. The *Privacy Act* provides them with the right to access their personal information held by the government and protection of that information against unauthorized use and disclosure. Ministers and department heads are responsible for ensuring that they are in compliance with each of these pieces of legislation.

In October 2010 the Office of the Privacy Commissioner (OPC) released a report in response to a complaint alleging Veterans Affairs Canada's (VAC or the Department) mishandling of a Veteran's personal information. The Privacy Commissioner concluded the Department was not compliant with federal privacy legislation and lacked the controls to protect sensitive information from being widely disseminated within the Department. The OPC made the following four recommendations to help the Department in addressing the issues noted in its report. The Department should:

1. Take immediate steps to develop an enhanced privacy policy framework with adequate protections and controls to regulate access to personal information within the department.
2. Revise existing information-management practices and policies to ensure that personal information is shared within the department on a need-to-know basis only. Personal information, including but not limited to sensitive medical information, should not be shared with programs that have no operational requirements for access to such information.
3. Provide training for employees about appropriate personal information-handling practices.
4. Review procedures to ensure that consent is obtained prior to personal information being transferred to veterans' hospitals.

In response to the OPC report, and at the Minister's request, the Department prepared a ten-point action plan specifically outlining the steps being taken. Item nine of the action plan was to conduct an independent annual assessment of the Department's compliance with the *Access to Information Act* and *Privacy Act* (the Acts).The Department engaged Audit Services Canada (ASC) to conduct this first annual assessment of the Department's compliance with the Acts.

Assessment Objective

The objective of this assessment was to assess the Department's compliance with the *Access to Information Act* and the *Privacy Act.*

The criteria used to assess compliance with the Acts and their sources are listed at Appendix A. Management agreed to the suitability of these assessment criteria.

Assessment Scope and Approach

This was an assessment, not an audit, and therefore the engagement was not designed or performed to provide a high level of assurance. Our assessment approach consisted of inquiry, review of documents, and analysis to gather point-in-time evidence of the Department's compliance with the Acts.

Our assessment was directed at the sections of the Acts for which the Department has responsibility. For the *Access to Information Act*, this included: Access to Government Records; Exemptions; Third Party Intervention; and annual reporting to Parliament. For the *Privacy Act*, this included: Collection, Retention, and Disposal of Personal Information; Protection of Personal Information; Personal Information Banks; Personal Information Index; Access to Personal Information; Exemptions; and annual reporting to Parliament.

Our assessment scope did not include the Regulations[1] made pursuant to the *Access to Information Act* and the *Privacy Act*. These Regulations contain information describing how certain sections of the Acts are to be applied. We did not assess compliance with the Acts at this level of detail.

At the Department's request, we expanded our scope to assess the status of each item in the ten-point action plan.

Our findings apply to the period during which we conducted our assessment, April 1 to May 31, 2011. Many changes took place and new policies and procedures were introduced in April 2011. In those areas, our findings are limited to whether the policies and procedures are well designed to deliver services in compliance with the Acts.

[1] *Access to Information Regulations* and *Privacy Regulations*

Assessment Findings Summary

The Department has worked to reduce the risk of a future privacy breach by introducing policies and procedures to prevent and detect the misuse of clients' personal information by its employees. Employee education and training are now critical to successful implementation of the new policies and procedures.

Given the recent implementation of these changes, we could not yet assess the effectiveness of the policies and procedures in achieving compliance with the Acts.

Summary results for the assessment criteria are presented at Appendix B.

Since October 2010, the Department has worked diligently to complete its 10-point action plan. Nine of the ten action plan steps were substantively completed at May 31, 2011. Five steps were fully completed and five were ongoing. Ongoing actions were primarily related to employee training and monitoring.

The Department plans to complete all actions prior to the Privacy Commissioner's audit, anticipated in fall 2011.

The implementation status of the action plan is presented at Appendix C.

Assessment Findings

Access to Information Act

The criteria used to assess compliance with the *Access to Information Act* and our related findings and recommendations are detailed below.

Criterion 1-1 — The Department responds to requests accurately and completely, providing timely access to records in the format requested.

As a result of our document review and interviews, we found that:

1. The Department developed policies and procedures for processing requests for access to records under the *Access to Information Act* to allow the Department to respond to requests accurately and completely and provide timely access to records in the format requested.
2. The policies and procedures make level-3 managers (and higher) responsible for providing accurate and complete information in response to a request. The responsible manager must complete an Access to Information Response form, confirming that the records provided are complete and accurate; that records can be released in their entirety; identifying areas that may require exemptions; and indicating if there are no records available.
3. The policies and procedures make the ATIP officer responsible for administration of the request for records. They prepare a detailed request for the ATIP liaison officer and, when the records are returned, the ATIP officers verify that the records are responsive to the request and apply exemptions in accordance with the Act, where required. Once the ATIP officer is satisfied that the request is complete, the records and a letter are sent to the requester with the goal of meeting the 30-day requirement stipulated in the Act. The Department's procedures are similar to the general ATIP process outlined at Appendix D.
4. Each area within the Department has its own ATIP liaison officer(s) and requests can require several liaison officers to obtain records identified. For example, requests concerning the Department's hospital required that the liaison officers in various areas of the hospital be contacted to retrieve records required. We noted one such request that took 174 days to complete as the ATIP officer contacted each area repeatedly to make certain the information provided was complete.
5. The Department has tools to help ensure the institutions are completing requests accurately, completely, and that access is provided on time. Examples of tools the Department uses include:
    - Action checklist – used on all ATI request files where the ATIP officer records the requester, case file number, due date of the request, and ATIP officer responsible. It also requires ATIP officers to confirm they have created an acknowledgement or transfer letter, identified what institutions may have records related to the request, other types of records that might be associated with the request, file email messages, and updated the AccessPro Case Management System, which is the electronic system used by the ATIP coordinator to track all activities related to a request.

- Access to information response form – requires level-3 managers, or higher, to sign-off that the records provided by the ATIP liaison officer to the ATIP officer are complete and accurate. This is to ensure that the manager is aware of the request and that all records related to the request were provided.
- Impact statement – requires the exemptions being applied to include a rationale supporting the recommended exemption cited in the Act.

6. There were 69 *access to information* requests outstanding in 2010-11 that were carried forward to 2011-12.

Criterion 1-2 — The Department twice a year confirms that its list of records and manuals is accurate, complete, and up to date.

As a result of our document review and interviews, we found that:

7. Annually, the Department is required to publish a description of its organization, responsibilities, programs and activities, the classes of records under its control, the personal information found within those classes of information, a list of the manuals used by employees in administering or carrying out institutional programs, and activities that affect the public; and a contact for access to information and privacy requests. The information is published in a legislated publication titled Info Source, a Treasury Board of Canada Secretariat website, that's primary purpose is to assist individuals exercise their rights under the *Access to Information Act* and the *Privacy Act*.
8. The Department submitted information to the Treasury Board Secretariat during the year to update the publications listed on Info Source.

Criterion 1-3 — The Department responds to requests for access to records as required and within the stipulated timelines.

As a result of our document review and interviews, we found that:

9. The *Access to Information Act* requires the Department to notify the requester in writing whether they will be given access to the records and to provide access within 30 days of receipt of the request. The Department sends an acknowledgement letter notifying the requester that the Department has received the request and has begun work on completing the request.

10. For purposes of understanding and assessing the process, we reviewed three requests submitted under the *Access to information Act* and found:

    - The Department telephoned one requester the day the request was received to clarify the records being requested. This resulted in the Department notifying the requester that they did not need to make a request under the *Access to Information Act* to obtain

the records they were seeking. The ATIP officer referred them to the National Client Contact Centre.

- The Department answered one request within six days of its receipt.
- The Department completed one request more than 150 days after the initial request was received. Consultation with another government department was required before the request could be completed. A letter was sent to the client notifying them that it would take more time to complete the request due to the nature of the records being requested. The letter notified the requester that they were entitled to contact the Information Commissioner and file a complaint.

11. The 2010–11 draft of the Annual Report on the Administration of the *Access to Information Act* indicated the Department responded to 60 percent of requests within 30 days of their receipt and, on files where an extension was taken, 73 percent of requests were completed on time. The Department received 148 formal requests which is a 7 percent increase over the previous year.

Criterion 1-4 — The Department applies exemptions to the disclosure of records in accordance with the Act.

As a result of our document review and interviews, we found that:

12. For purposes of understanding and assessing the process, we reviewed three requests submitted under the *Access to Information Act* and found that the Department applied exemptions to one of the requests. The sections cited in the file were:
    - 19(1) – information was redacted because it contained personal information of an individual other than the requester;
    - 21(1)(b) – information was redacted because it related to an account of consultation and debriefings involving officers or employees of a government institution; and
    - 23 – information was redacted because it was subjected to solicitor-client privilege.
13. The 2010–11 draft Annual Report on the Administration of the *Access to Information Act* identified 111 cases where formal requests had exemptions applied. These included the sections mentioned above as well as sections 14, 15, 16, 18, 20 and 22 of the *Access to Information Act*.
14. The *Policy and Procedures for the Processing of requests for Access to Records and Personal Information under the Access to Information Act and the Privacy Act* provides guidelines on the application of exemptions under the *Access to Information Act*. The authority to apply the exemptions as outlined in the delegation of authority rests with the ATIP officer. However, an institution providing records is required to review the records and highlight the information they recommend exemptions be applied to. The ATIP officer decides whether the information highlighted requires exemption, and if other parts of the records also require exemption. The Department also requires that an impact statement form

be completed by the providing department justifying the reason for the disclosure or protection of the information.

Criterion 1-5 — The Department provides third parties with notice that it intends to disclose a record.

As a result of our document review and interviews, we found that:

15. The Department uses a standard letter to notify third parties of its intent to disclose a record. The letter states, 'Although we have reason to believe that these records may contain third-party information as described in Section 20(1) of the *Access to Information Act*, we do not have sufficient information in our files to substantiate this. Thus, as required by the Act, we intend to disclose the records on (date)…If you have any concerns with the disclosure of these records, please make written representations to the undersigned as to why portions of the records should not be disclosed. If you have not responded by (Date), the records will be disclosed.' We found that the need to notify third parties occurs infrequently.

Criterion 1-6 — The Department prepares an annual report on the administration of the Act to be tabled in Parliament within three months of year end.

As a result of our document review and interviews, we found that:

16. The Department prepared its 2010–11 Annual Report on the Administration of the *Access to Information Act* in May 2011. The Report must be submitted to each House of Parliament within three months from the financial year end or, if Parliament is not sitting, within 15 days of the next session. At the time of our report completion, the deadline had not passed and the Report had not been submitted.
17. The 2009–10 annual Report was deposited with the Clerk of the House October 19, 2010. The House was not sitting the end of June when the Report was due and it resumed its session September 20, 2010. The Report was submitted 29 days after the House returned for the third session of the 40th Parliament.

Privacy Act

The criteria used to assess compliance with the *Privacy Act* and our related findings and recommendations are detailed below.

Criterion 2-1 — The Department collects, retains, and disposes of personal information in accordance with the *Act*.

As a result of our document review and interviews, we found that:

18. The Department implemented a *General Privacy Policy and Guidelines for the Collection Creation, Management, and Handling of Personal Information* March 31, 2011. This document is available on the Department's intranet site.
19. The Department collects data for the various programs and services it delivers to its clients. The Department controls the types of information collected by using forms which specify the information to be gathered. The forms used to gather information are completed either by the client, staff or a third party. Some of these forms are completed in person at a district office, through client MyVac accounts, by nurses, and by individuals who have been given power of attorney on behalf of a client.
    - The Department is reviewing its forms to make certain they meet the need-to-know requirement of the *Privacy Act* and that the Department is not inadvertently collecting information it does not require for a specific client purpose. The Department now requires that any new forms used to gather information are first reviewed by IM advisors and approved by the IM Director to confirm they comply with legal and technical authorities.
    - Forms used by nurses require a more general approach to collecting information when they are performing a client assessment. Nurses are therefore provided with privacy training on what is considered acceptable information and what is considered to be excess information.
    - For the purposes of understanding and assessing the collection of information, we reviewed a sample of forms and noted they contained a statement identifying the reason for the collection of personal information and a statement that it is protected under the *Privacy Act* from unauthorized disclosure.
20. Areas within the Department are responsible for ensuring the records retained are up-to-date. The Veterans Independence Program, for example, performs annual reviews and client screenings to confirm that records are correct. These reviews involve contacting clients and verifying information based on a questionnaire.
21. Records may also be verified when clients contact the Department. Client screenings are conducted from a prepared list of questions.
22. The Department has a Records Disposition Authority issued by Library and Archives Canada allowing it to dispose of records no longer required. This is currently being applied to paper documents. It cannot, however, be applied to electronic records until the Department implements an electronic documents and records management system.

23. The complexity of CSDN's design prevents the Department from removing electronic records in an efficient manner.

Criterion 2-2 — The Department protects its personal information.

As a result of our document review and interviews, we found that:

24. In response to the recommendation from the Office of the Privacy Commissioner, the Department developed a Privacy Framework which was implemented on April 1, 2011. The Framework creates awareness and provides guidance with respect to information management and privacy practices. The framework comprises the:

    - *General Privacy Policy and Guidelines for the Collection, Creation, Management, and Handling of Personal Information.* This document is the main component of the Department's Privacy Framework.
    - *Veterans Affairs Canada Privacy Protection Infrastructure.* This document outlines the responsibilities of the newly created position of Chief Privacy Officer (CPO) and the new Departmental Privacy Committee (DPC). The CPO's responsibility is to provide strategic leadership and oversight on privacy issues. The DPC, chaired by the CPO, reviews risk management and privacy compliance, and establishes privacy priorities and measures.
    - *Information Management Policy, Veterans Affairs Canada Information Management Best Practices, and IM & Privacy Directive on Email.* This document provides guidance on effective information management.
    - *Privacy Breach Policy and Privacy Breach Guidelines.* Provide information in terms of objectives and definitions. This document provides roles and responsibilities of specific positions within the Department and on actions to be taken if there is a privacy breach.

25. The Department established a Matrix Review Committee to evaluate who should have access to CSDN. Questionnaires, developed by the Matrix Review Committee of the IT/IM Directorate, were sent to units within the Department to obtain information related to employees' need to access the system. An Access Contact was responsible for working with managers or supervisors to document the rationale for each CSDN access level essential for the employee to carry out their required job functions. The Functional Authority for each level approved or denied the access, often only after clarifying and questioning the rationale provided. An example of a completed questionnaire including sample rationales was provided to CSDN Access Contacts and managers. These sample rationales included, 'Access level 3 required to view all client information with the exception of payment information and pension history' and 'Access level 67 not required because we do not have to see what a veteran has done online'. The head office review of positions was completed and changes are being implemented. The 2800–3000 system users were reduced by approximately 400. The regional reviews are not expected to be completed until September 2011.

26. A preliminary review of the Department's IM/IT environment undertaken in November 2010 by an expert from FINTRAC resulted in a number of recommendations. Considered

highest in priority were those related to the reporting database (RDB), which contains information from the operational databases and is accessible by over 100 users within the Department. The recommendations were:

- **Reassess information gathering with a privacy lens**. The Department determined that creating additional reports without identifiers in a parallel catalog would not be an effective solution. Instead, privacy training for the system's frequent users will be implemented.
- **Review and ensure operational reports posted do not contain personal information.** Since the resources needed to change the format of existing reports are not available, the operational reports will be reviewed as they come up for renewal.
- **Enhance RDB audit capabilities**. An audit program was implemented capturing user activity.
- **Review user access and enhance for smaller subset reporting**. The Department reviewed and verified RDB users but was unable to limit the extent of access because of the nature of the database. They are looking for another solution.

27. FCHPS, a benefits payment system contracted to Medavie Blue Cross, is defined to be under the Department's control. The Department has access control policies and procedures in place to manage access by its employees. For Medavie Blue Cross employees who have access to the system and related client information, data modifications and authentication events are logged and recorded for audit purposes. Read-only inquiries into client information are not reported for audit purposes. According to Medavie Blue Cross, access to the system is reviewed on an annual basis and 'need to know' is part of its overall access control process.
28. In October 2010 the Department began monitoring access to CSDN to verify that employees have a need-to-know reason for accessing client files. The emphasis is on read-only accesses. Emails were originally sent to managers advising them of employee access but there was slow or limited response. Emails are now sent directly to employees advising them that their access to a specific client notebook was detected and they are required to provide a legitimate reason to access the file. If employees fail to respond their supervisor is advised. Related to the CSDN monitoring initiative, we found:
    - There are 9 million CSDN accesses per year or 30,000 per day. IT Security staff indicated that even with the monitoring initiative, the number of accesses has remained the same since October.
    - Monitoring has raised employee awareness; however, employees are now apprehensive knowing that every file access is monitored.
    - There are limitations to the monitoring as CSDN does not track the time that an employee spends in a client file.
29. The Department drafted a *Protocol for the Use of Personal Information for Non-Administrative Purposes* to be used for research, audit, and related activities.
30. The *VAC Discipline Policy and Disciplinary Guidelines* state that because of the nature of the Department's mandate and the highly personal information in its possession,

inappropriate access to client files and inappropriate disclosure of client information are types of misconduct which could warrant disciplinary measures. The *Discipline Policy and Disciplinary Guidelines* are available on the Department's intranet.

31. The Department has corporate files that contain personal information but lacks systems to manage this information. The Department has developed an employee guidance document, *Personal Information as Supporting Documentation on Departmental Subject Records.* Its purpose is to provide direction on acceptable use of personal information as supporting documentation on departmental subject records.
32. In addition to electronic client records, hard-copy records containing client information are maintained at head office as well as regional offices. At the Centralized Processing Centre hard-copy client files are kept in unlocked storage until the client file is no longer active. Operational practices require that portions of client files be copied and forwarded to the Finance Directorate (e.g., Earnings Loss Program files).
33. During the collection of client data for program use, the Department ensures it obtains signed authority to release information and maintains this authority on file. The forms used contain the client name and file number as well as information on the party to whom information will be released and the nature of the information. This allows the Department to consult with community service providers and other health professionals in the managing of a client file.
34. The Department developed *Guidelines on Handling Personal Information in the Preparation of Briefing Materials.* Despite the Privacy Awareness Training, a departmental review of briefing notes revealed that between November 1, 2010 and March 31, 2011, 30 percent of briefing notes and 28 percent of ministerial reports contained more than 'need-to-know' information.
35. Privacy Impact Assessments (PIAs) assess privacy risks related to programs and activities. PIAs and threat and risk assessments, if required, are now completed before any changes to programs or new programs are implemented. There are a number of legacy programs for which PIAs have not been completed as they were in place before this requirement. The Access to Information and Privacy (ATIP) Coordinator for VAC has primary responsibility for the conduct of PIAs.
36. The Department produced or is producing a number of guidance documents related to the disclosure of personal information in accordance with section 8 of the Act. These include guidelines for the disclosure of information to the Attorney General of Canada; Policing Services and Federal Investigative Bodies; Subpoena, Warrant, or Court Order; and to Ministers and Members of Parliament.

Criterion 2-3 — The Department verifies that its personal information banks are complete.

As a result of our document review and interviews, we found that:

37. The Department submits new or revised personal information banks (PIBs) to the Information and Privacy Policy Division of the Treasury Board Secretariat where the

content is reviewed for compliance with the *Privacy Act*. PIBs are then to be input to Info Source.

Criterion 2-4 — The Department annually confirms that its personal information bank index is accurate, complete, and up to date.

As a result of our document review and interviews, we found that:

38. The Department submitted its most recent listing of PIBs to TBS to be included in the 2010 edition of Info Source which will update the 2009 edition currently available.
39. The latest submission included a number of revised PIBs containing updated information approved by TBS. PIBs are reviewed and updated as often as possible in consultation with the program areas to ensure new collections, uses, and disclosures are reflected in the PIBs. Each time changes are made, TBS approval is required.
40. The Department's 2009 PIB Index includes all of the information required by TBS and the *Privacy Act*.

Criterion 2-5 — The Department responds to requests for access to personal information as required and within the stipulated timelines.

As a result of our document review and interviews, we found that:

41. The *Privacy Act* requires that the Department provides notice to the requestor within 30 days that the documents will be provided and access will be given.
42. For purposes of understanding and assessing the process, we selected three requests submitted under the *Privacy Act* and found:
    - The Department answered one request in three days.
    - The Department completed one request in 30 days.
    - The Department completed one request in 121 days. This request contained 1,286 pages of documents and 2 cassette tapes. We could not confirm the requester was notified that the response would exceed 30 days, as required by the Act, section 15.
43. The draft of the 2010 - 2011 Annual Report on the Administration of the *Privacy Act* indicated the Department responded to 69 percent of requests within 30 days of receipt and, when extensions were taken, 70 percent of requests were completed on time.
44. There were 96 formal privacy requests outstanding in 2010-11 that were carried forward to 2011-12.

Criterion 2-6 — The Department applies exemptions to the disclosure of personal information in accordance with the Act.

As a result of our document review and interviews, we found that:

45. For purposes of understanding and assessing the process, we reviewed three requests submitted under the *Privacy Act* and found the Department applied exemptions in each case. They each referenced the *Privacy Act*, section 26 requiring personal information of another individual, other than the requester, be removed from the records. When the Department completes a request it sends a letter to the requester along with the records requested and cites the sections of the Act applied. As well, for any portion of the records that was redacted, the section of the Act applied is noted next to the redacted area.
46. The draft 2010-2011 Annual Report on the Administration of the *Privacy Act* identified 170 cases where exemptions were applied for formal requests. These included the sections mentioned above and sections 22, 27 and 28 of the *Privacy Act*.
47. The *Policy and Procedures for the Processing of Requests for Access to Records and Personal Information under the Access to Information Act and the Privacy Act* provides guidelines on applying exemptions in the *Privacy Act*. The authority to apply the exemptions has been delegated to the ATIP officer. However, the institution providing the records is required to review the records and highlight the information they believe requires exemptions to be applied. The ATIP officer reviews the records and makes the decision whether the information highlighted qualifies for exemption or if other parts of the records require exemptions.

Criterion 2-7 — The Department prepares an annual report on the administration of the *Act* to be tabled in Parliament within three months of year end.

As a result of our document review and interviews, we found that:

48. The Department prepared its 2010–11 Annual Report on the Administration of the *Privacy Act* in May 2011. The Report must be submitted to each House of Parliament within three months from the financial year end or, if Parliament is not sitting, within 15 days of the next session. At the time of our report completion, the deadline had not passed and the Report had not been submitted.
49. The 2009–10 annual Report was deposited with the Clerk of the House October 19, 2010. The House was not sitting the end of June when the Report was due and it resumed its session September 20, 2010. The Report was submitted 29 days after the House returned for the third session of the 40th Parliament.

Recommendations

1. Management should select and implement an electronic documentation and records management system to control its corporate information holdings, including any personal information that may be held there.
2. Management should provide ongoing education and training to employees on the intent and application of policies and procedures comprising the Department's new Privacy Framework.
3. Management should implement systems so that records can be disposed of in accordance with its Records Disposition Authority from Library and Archives Canada.
4. The Chief Privacy Officer should continuously monitor and report on the Department's compliance with its Privacy Framework and the *Privacy Act*.

Appendix A — Assessment Objective, Criteria, and Source

Objective	Criteria	Source
To assess the Department's compliance with the *Access to Information Act* and the *Privacy Act*	1-1 VAC responds to requests accurately and completely, providing timely access to records in the format requested	*Access to Information Act*, section 4
	1-2 VAC twice a year confirms that its list of records and manuals is accurate, complete, and up to date	*Access to Information Act*, section 5
	1-3 VAC responds to requests for access to records as required and within the stipulated timelines	*Access to Information Act*, sections 6-12
	1-4 VAC applies exemptions to the disclosure of records in accordance with the *Act*	*Access to Information Act*, sections 13-26
	1-5 VAC provides third parties with notice that it intends to disclose a record	*Access to Information Act*, section 27
	1-6 VAC prepares an annual report on the administration of the *Act* to be tabled in Parliament within three months of year end	*Access to Information Act*, section 72
	2-1 VAC collects, retains, and disposes of personal information in accordance with the *Act*	*Privacy Act*, sections 4-6
	2-2 VAC protects its personal information	*Privacy Act*, sections 7-9
	2-3 VAC verifies that its personal information banks are complete	*Privacy Act*, section 10
	2-4 VAC annually confirms that its personal information bank index is accurate, complete, and up to date	*Privacy Act*, section 11
	2-5 VAC responds to requests for access to personal information as required and within the stipulated timelines	*Privacy Act*, sections 14-17
	2.6 VAC applies exemptions to the disclosure of personal information in accordance with the *Act*	*Privacy Act*, section 18-28
	2.7 VAC prepares an annual report on the administration of the *Act* to be tabled in Parliament within three months of year end	*Privacy Act*, section 72

Appendix B — Assessment Criteria Matrix

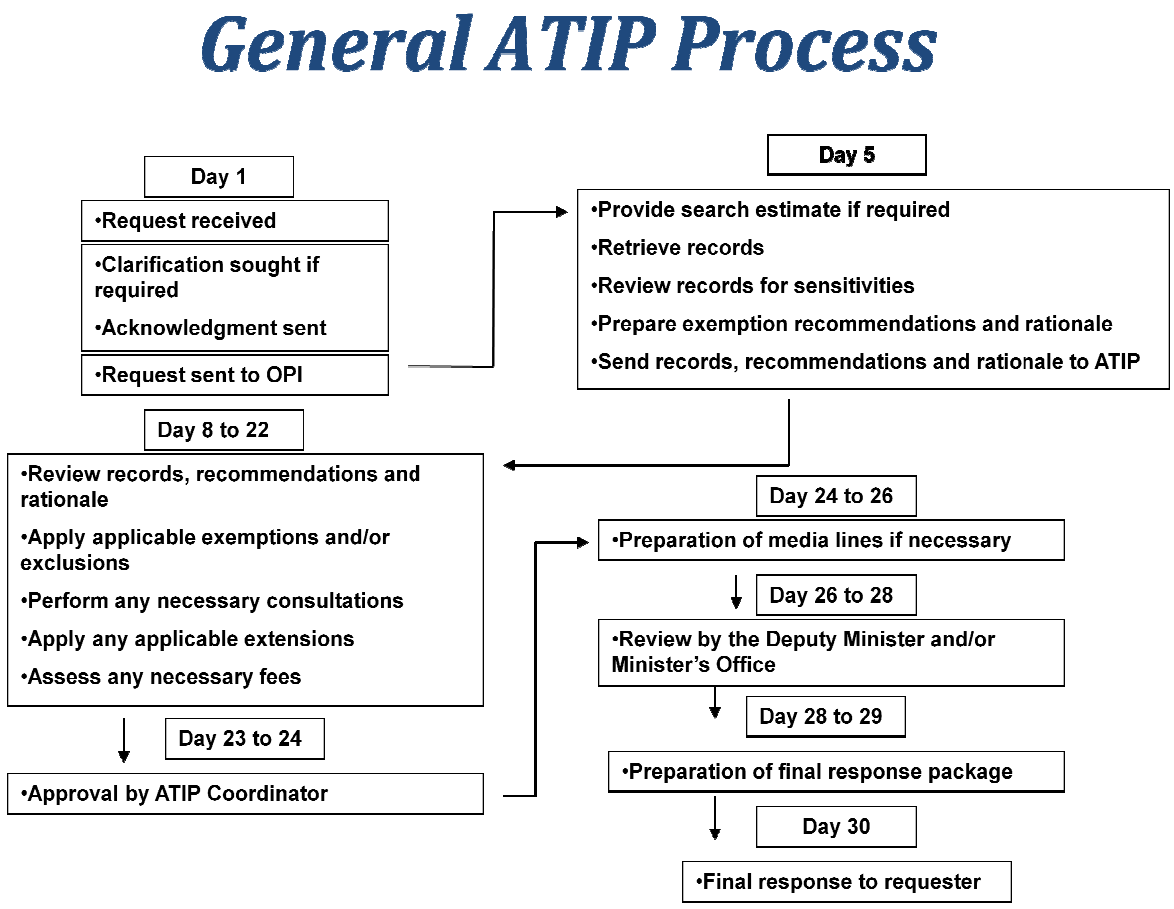
Assessment Criteria	Met	Partially Met	Not Met
Access to Information Act			
1.1 VAC responds to requests accurately and completely, providing timely access to records in the format requested.	X		
1.2 VAC twice a year confirms that its list of records and manuals is accurate, complete, and up to date.	X		
1.3 VAC responds to requests for access to records as required and within the stipulated timelines.		X	
1.4 VAC applies exemptions to the disclosure of records in accordance with the *Act*.	X		
1.5 VAC provides third parties with notice that it intends to disclose a record.	X		
1.6 VAC prepares an annual report on the administration of the *Act* to be tabled in Parliament within three months of year end.	X		
Privacy Act			
2.1 VAC collects, retains, and disposes of personal information in accordance with the *Act*.		X	
2.2 VAC protects its personal information.	X		
2.3 VAC verifies that its personal information banks are complete.	X		
2.4 VAC annually confirms that its personal information bank index is accurate, complete, and up to date.	X		
2.5 VAC responds to requests for access to personal information as required and within the stipulated timelines.		X	
2.6 VAC applies exemptions to the disclosure of personal information in accordance with the *Act*.	X		
2.7 VAC prepares an annual report on the administration of the *Act* to be tabled in Parliament within three months of year end.	X		

Appendix C — Ten-Point Action Plan Assessment

Action Step	Description	Target Date	Status
1. Review system access in detail	Detailed review of 2,800 CSDN user accounts	March 31, 2011	**Ongoing.** Initial assessment of CSDN access matrix in November 2010 resulted in 400 user accounts removed; Matrix Review Committee created. Survey of access requirements to be completed September 2011. Plan to implement regional access control.
2. Communicate discipline policy	A strengthened discipline policy and guidelines with clear sanctions developed and communicated to staff	October 31, 2010	**Completed.** Discipline guidelines posted on Department's intranet with email notification to employees, May 2011.
3. Introduce a privacy lens for briefing note process	New procedures on the appropriate use of client information when preparing briefing notes and other documents for use within the Department	October 31, 2010	**Completed.** New briefing notes guideline provided to level-3 managers. Also new guidelines for disclosure of information to Members of Parliament.
4. Appoint external systems expert	External experts in electronic information systems management to review and recommend changes to departmental systems	October 31, 2010 to March 31, 2011	**Completed.** Expert reviewed IM/IT systems in November 2010 and made 16 recommendations for improvement.
5. Appoint external privacy expert	A team of experts in government information management and privacy to review and recommend changes to departmental processes to ensure information is protected and access is controlled	October 19, 2010 to March 31, 2011	**Completed.** Three experts engaged to review ATIP policies and procedures; provide ATIP oversight and guidance; and provide training for managers.
6. Enhance monitoring of electronic systems	A team to proactively monitor, review, and investigate who is accessing client information. Where access is inappropriate, disciplinary measures to be taken	October 18, 2010	**Ongoing.** CSDN access monitored by IT Security since January 2011; daily reports prepared. Employees receive an email asking for an explanation of why the account was accessed.
7. Provide mandatory privacy training	A mandatory privacy awareness program for all staff launched October 19, 2010. This program covers 'need to know', client consent when sharing information, and the range of disciplinary measures that will be taken if privacy is breached. Ste. Anne's Hospital has its own programs related to privacy and confidentiality of client information	October 19, 2010 to November 19, 2010	**Ongoing.** 82% of staff trained on need-to-know requirements of Privacy Policy in October-November, 2010. This training is now included in VAC's information management course and the MOP/SOP sessions to begin in June 2011. Need-to-know training is also offered to students and new employees of the Department.

Action Step	Description	Target Date	Status
8. Provide in-depth training on Government privacy policies and procedures	In-depth training for all staff on new policies, guidelines, and procedures	January – March 31, 2011	**Ongoing.** All managers trained in March 2011. Sessions also held for regional offices. Training covered Privacy Management Framework, policies, and guidelines. Commitment to train all staff by July 2011.
9. Conduct independent annual assessment	An annual independent assessment of VAC's compliance with the Privacy Act and Access to Information Act	Annually, starting June 2011	**Completed.** Audit Services Canada engaged to conduct annual assessment; report in June 2011.
10. Prepare for Privacy Commissioner's audit	The Department has started preparations for a comprehensive audit by the Privacy Commissioner	Immediately	**Ongoing.** All steps above are in preparation for the Privacy Commissioner's audit.

Appendix D — General ATIP Process Diagram



Prepared by Audit Services Canada