Agriculture and Agri-Food Canada | Agriculture et Agroalimentaire Canada

Audit of Information Privacy

Final Report

Office of Audit and Evaluation

November 2010

Canada

The AAFC Audit Committee recommended this audit report for approval by the Deputy Minister on November 5, 2010.

To obtain more information on the Office of Audit and Evaluation, please visit:
http://www.agr.gc.ca/aud_eval

AAFC 11426E
ISBN 978-1-100-18260-5
Cat. No. A34-18/2011E-PDF

Aussi offert en français sous le titre : Protection des renseignements personnels

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the course of its program delivery, and its provision of services to Canadians, AAFC collects and manages extensive amounts of personal information on its clients and its staff members. In doing so, the Department is subject to the *Privacy Act* and related policies and directives issued by the Treasury Board Secretariat (TBS). In delivering its programming, and due to the nature of its work, AAFC faces an inherent risk of violating requirements of the *Privacy Act* or TBS policies and directives. The importance of privacy-related risk mitigation activities is also noted in AAFC's Corporate Risk Profile.

The Access to Information and Privacy (ATIP) Office in AAFC reports through Information Management Services (IMS) and the Information Systems Branch (ISB) and has the mandate to implement and administer both the *Access to Information Act* and the *Privacy Act*. The ATIP Office is responsible to ensure the appropriate policy framework, processes, and tools have been implemented at AAFC to ensure adherence to privacy requirements. Given the management of personal information takes place at the program level, program staff members also have significant responsibilities to ensure the appropriate implementation of this central direction regarding the management of personal information.

In light of the inherent risks associated with adhering to the *Privacy Act* in an environment such as AAFC's, the Deputy Minister approved an audit of *Privacy Act* compliance to be included in the 2009-12 AAFC Risk-Based Audit Plan.

The objective of the audit was to assess the adequacy and effectiveness of the management control framework in place to support compliance with the *Privacy Act* and related Treasury Board policies and directives.

The scope of the audit included all personal information, whether related to clients or staff members of AAFC and whether in electronic or paper format. The audit encompassed AAFC's activities related to privacy compliance from April 1, 2008 to March 31, 2010. The audit planning and conduct phases were completed between November 2009 and April 2010.

The audit criteria used to assess the management control framework were developed based on AAFC's legislative and policy requirements related to privacy.

The conclusion of the audit is that AAFC's current privacy management control framework requires moderate improvements to address certain deficiencies which expose AAFC to the potential of non-compliance with the *Privacy Act* and related Treasury Board polices and directives and increase the risk of the inappropriate collection, use, or disclosure of personal information. Issues were noted in the following areas:

- A governance body has not been clearly mandated to provide privacy oversight and roles and responsibilities outside of the ATIP office have not been clearly identified;

- A privacy training and awareness strategy has not been developed to ensure that the privacy requirements of key positions across AAFC are understood by their incumbents;
- There is a lack of controls to ensure the appropriate management of personal information by third party delivery agents;
- There is a lack of controls to ensure the uses of the Social Insurance Number (SIN) reflect the requirements of the TBS Directive on the Use of the SIN;
- Privacy risks have yet to be fully considered and integrated into the development of the AAFC Service Excellence Agenda;
- The review of Privacy Impact Assessments (PIAs) has not been timely and there has been a lack of follow-up to determine if risks have been appropriately mitigated; and
- Electronic information which may include personal information is generally not disposed of in accordance with records disposition schedules.

Controls in other areas were found to be satisfactory, with a number of good practices noted. For example, the ATIP Office has made significant progress in the last year in consolidating its role in the department and identifying the required resources to ensure its mandate can be achieved. This includes drafting a number of policies and developing privacy training and awareness for the department. The ATIP Office has also ensured the PIA process has become centralized and directed by the ATIP Office.

For the areas within the scope of the audit, including both program areas and the HR Branch, personal information is being collected within AAFC with the appropriate authority and with an appropriate purpose consistent with the administration of the program/functional area.

The Chief Audit Executive has provided assurance that sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided in the detailed report.

1.0 INTRODUCTION

1.1 Background

In the course of its program delivery, and its provision of services to Canadians, AAFC collects and manages extensive amounts of personal information on its clients and its staff members. In doing so, the Department is subject to the *Privacy Act* and related policies and directives issued by the Treasury Board Secretariat (TBS). The purpose of the *Privacy Act* is to protect the privacy of the personal information of individuals held by government institutions and to provide individuals with a right to access and correct that personal information. There are a number of TBS policies and directives related to the appropriate privacy practices of the Department, including specific Directives related to the use of the Social Insurance Number (SIN) and the conduct of Privacy Impact Assessments (PIAs). PIAs provide a risk-based framework for identifying and reviewing privacy issues related to programs, initiatives or systems that collect or manage personal information.

The Access to Information and Privacy (ATIP) Office in AAFC reports through Information Management Services (IMS) and the Information Systems Branch (ISB), headed by the Chief Information Officer (CIO), and has the mandate to implement and administer both the *Access to Information Act* and the *Privacy Act*.

The Office's *Privacy Act*-related responsibilities include ensuring that legislative and policy requirements are met and that an appropriate privacy management framework (PMF) has been implemented for the Department. The Office of the Privacy Commissioner of Canada (OPCC) defines a PMF as: "… *the way in which institutions organize themselves through structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and ensure compliance with the Privacy Act*." There are currently seven positions related to privacy within the ATIP Office.

In addition to the ATIP Office, the Centre of Program Excellence (COPE) within FFPB has an oversight role for all non-BRM (Business Risk Management) grant and contribution programs that includes providing guidance on the privacy provisions programs should include in agreements with third parties.

Finally, all AAFC staff members have a responsibility to protect the privacy of the personal information that they manage.

In delivering its programming, and due to the nature of its work[1], AAFC could face a high inherent risk of violating requirements of the *Privacy Act* or TBS policies and directives. The importance of privacy-related risk mitigation activities is also noted in AAFC's Corporate Risk Profile. In light of this risk, the Deputy Minister approved an audit of *Privacy Act* compliance to be included in the 2009-12 AAFC Risk-Based Audit Plan.

[1] For example, AAFC makes extensive use, through both transfer payments and contractual arrangements, of third parties, i.e. independent organizations or individuals, to deliver AAFC programs or services to intended beneficiaries or ultimate recipients.

1.2 Audit Objective

The objective of the audit was to assess the adequacy and effectiveness of the management control framework in place to support compliance with the *Privacy Act* and related TBS policies and directives.

1.3 Audit Scope

The audit assessed the management control framework and the governance arrangements in the Department to support compliance with the *Privacy Act* and related TBS policies and directives. The scope of the audit included all personal information, whether related to clients or staff members of AAFC, and whether in electronic or paper format. The audit encompassed AAFC's activities related to privacy compliance for the period from April 1, 2008 to March 31, 2010.

Based on the risk assessment performed during the planning phase of the audit, the areas selected for the focus of the audit in addition to the ATIP Office were the Farm Financial Programs Branch (FFPB) and the Human Resources (HR) Branch. The rationale for selecting these areas is that the majority of personal information related to clients is collected by FFPB, specifically the Farm Income Programs Directorate (FIPD) (based in Winnipeg) and the Finance and Renewal Programs Directorate (based in Ottawa), and a vast amount of potentially sensitive personal information on staff members is held by the HR Branch.

While the ATIP Office is also responsible to ensure compliance with the *Access to Information Act, c*ompliance with the *Act was* not within the scope of this audit.

1.4 Audit Approach

The audit was conducted in accordance with the *Standards for the Professional Practice of Internal Audit* and the Treasury Board *Policy on Internal Audit*. These standards require that the audit be planned and performed in such a way as to obtain reasonable assurance that audit objectives were achieved.

The audit included various tests, as considered necessary, to provide such assurance. These tests included interviews, observations, walkthroughs, review of supporting documentation, and analytical reviews.

The audit criteria used to assess the management control framework were developed based on AAFC's legislative and policy requirements related to privacy, specifically those outlined in:

- *Privacy Act* and associated regulations;
- Policy on Privacy Protection;
- Directive on the Social Insurance Number (SIN); and
- Privacy Impact Assessment (PIA) Policy.

Of note, the TBS PIA Policy has been replaced effective April 1, 2010 with a new PIA Directive. The new Directive provides a more risk-based approach to the requirement and depth of PIAs. A new Directive on Privacy Practices also came into effect April 1, 2010,

which further explains the requirements of the *Privacy Act* and the Policy on Privacy Protection.

The audit was completed in the following phases:

Planning – November 2009 to February 2010
Conduct – February 2010 to April 2010
Reporting – May 2010

1.5 Conclusion

It is the opinion of AAFC's Internal Audit Directorate that AAFC's current privacy management control framework requires moderate improvements to address deficiencies which increase the risk of the inappropriate collection, use, or disclosure of personal information and expose AAFC to the potential of non-compliance with the *Privacy Act* and related Treasury Board policies and directives.

Improvements in the management control framework are required in the areas of:

- governance and oversight of privacy;
- privacy training and awareness;
- the use of the Social Insurance Number (SIN);
- third party delivery agents' management of personal information; and
- the disposition of electronic personal information.

The deficiencies in these areas are detailed in Section 2.0.

Controls in other areas were found to be satisfactory, with a number of good practices noted, including:

- The ATIP Office has made significant progress in the last year on consolidating its role in the department and identifying the required resources to ensure its mandate can be achieved. This has included drafting a number of policies and developing and delivering privacy training and awareness sessions for the Department. The ATIP Office has also ensured the PIA process has become centralized and directed by the ATIP Office to provide consistency in the conduct of PIAs and in the management of common risks across programs.
- The ATIP Office is meeting its responsibilities under the *Privacy Act* related to the submission of Personal Information Banks (PIBs) to Treasury Board for inclusion in InfoSource and to the development of the *Annual Report on the Privacy Act to Parliament*.
- For the areas within the scope of the audit, including both program areas and the HR Branch, personal information is being collected within AAFC with the appropriate authority and with an appropriate purpose consistent with the administration of the program/functional area.

Leveraging the two new TBS privacy-related Directives should assist the ATIP Office in the further development and implementation of a risk-based approach to managing privacy within AAFC.

1.6 Statement Of Assurance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report.

The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The opinion is applicable only to the entity examined. The evidence was gathered in compliance with TB policy, directives and standards on internal audit, and the procedures used meet the professional standards of the Institute of Internal Auditors. The evidence has been gathered to be sufficient to provide senior management with the proof of the opinion derived from the internal audit.

Original signed by:

_____ _____

Chief Audit Executive Date

1.7 Acknowledgements

The Office of Audit and Evaluation would like to thank those individuals who contributed to this project and, in particular, departmental interviewees who provided insights and comments useful to this audit.

2.0 DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

This section presents the key observations, based on the evidence and analysis associated with the audit, and provides recommendations for improvement.

It is expected that responses will be provided by management and include:

- an action plan to address each recommendation;
- a lead responsible for implementation of the action plan; and
- a target date for completion of the implementation of the action plan.

2.1 Privacy Governance and Oversight

A governance body has not been clearly mandated to provide privacy oversight for the Department and roles and responsibilities for privacy have not been clearly defined for staff members outside of the ATIP Office.

To ensure it is compliant with the *Privacy Act* and related TBS policies and directives, AAFC is required to implement the appropriate structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks and ensure compliance with privacy requirements.

Roles and responsibilities related to privacy within AAFC have not been formally defined and communicated. AAFC is currently drafting a Privacy Management Framework (PMF) intended to clarify roles and responsibilities, however, the draft PMF is only in its initial stages and, while it outlines the roles and responsibilities of the ATIP Office and senior management, it does not specifically outline the roles and responsibilities of program managers or other staff that manage personal information. Once finalized, the PMF needs to be appropriately communicated so that all staff members understand their roles and responsibilities related to privacy.

The Business Information System Committee (BISC) has served as a de facto privacy governance body, e.g. as part of yearly IM/IT reporting and planning, ATIP presented to BISC on its priority areas and on the AAFC Privacy Breach Policy. It should be noted, however, that privacy oversight and governance activities, such as consideration of important/systemic issues arising from PIAs or privacy breaches, have not been specifically tasked to BISC. This has also contributed to a lack of guidance and direction on emerging privacy issues related to the Department's plans and priorities, such as those related to the use of third party delivery agents (refer to Section 2.3).

With a lack of established roles and responsibilities and central direction, program areas have been left to incorporate their own privacy requirements into program-specific procedures and processes. For example, the Farm Income Programs Directorate (FIPD) has developed Contact Centre Guidelines related to the handling of privacy issues with callers while the Advance Payment Program (APP) has taken a number of Privacy related initiatives, including developing their own privacy policy, surveying administrators' privacy

practices, updating their Program Officer Desktop Procedures manual and developing a set of privacy review questions to be incorporated into their compliance visit check list.

Recommendation 1:

The Chief Information Officer should:

I. Finalize a Privacy Management Framework (PMF) for the Department that outlines the required privacy roles and responsibilities for all staff members throughout the department (particularly those responsible for program delivery), designates a specific governance body with responsibility for privacy, and outlines the specific policy guidance required to be provided from the ATIP Office.
II. Develop a Privacy Policy for AAFC that is tied to federal government legislative and policy requirements but reflects the nature of AAFC operations; and
III. Establish a formal plan to actively offer assistance to program areas in ensuring that their specific procedures and processes are consistent with privacy requirements, as outlined in the PMF and the Privacy Policy once they are established.

Management Response:

The CIO agrees with the three components of recommendation 1.

Action Plan:

I. A Privacy Management Framework is in the approval process with senior management.

II. A Privacy policy has been drafted. The policy will be completed once TBS has issued its final guidance on its recently revised privacy policy suite.

III. A formal plan will be established once the Privacy Management Framework and Privacy Policy documents are complete and existing activities will continue to be evaluated.

Lead Responsible: CIO

Target Dates for Completion:

I. October 2010
II. October 2011
III. October 2011

2.2 Privacy Training and Awareness

Although there is general awareness of privacy requirements within AAFC, the specific requirements related to an AAFC staff member's day to day job function are less well understood.

The Department is responsible for making its employees aware of policies, procedures and legal responsibilities under the Act. In spite of the ATIP Office having made significant progress related to privacy training and awareness (e.g. the Office has developed and is providing privacy training each month, including a brief presentation during orientation sessions to new AAFC employees, and has also developed training sessions on PIAs and privacy breaches), the privacy training in the last two fiscal years has been delivered to approximately only 5% of AAFC employees and only a handful of AAFC employees have taken the PIA training.

The current training provided by the ATIP Office contains high level principles relating to privacy, but does not specifically outline the requirements of the *Privacy Act* or Treasury Board policies and directives in relation to how AAFC staff members manage personal information. A privacy training strategy has not been developed to target the training at those positions within AAFC that represent a higher inherent privacy risk based on their roles/responsibilities.

Given the current small number of AAFC staff that have been trained, and the fact that the training sessions are not mandatory and are high level in nature, there is an increased risk that personal information may be inappropriately managed.

Recommendation 2:

The Chief Information Officer (CIO) should:

I. Develop a needs and risks based privacy training strategy.
II. Modify the privacy awareness section of current privacy training sessions to focus on practical guidance/checklists highlighting how *Privacy Act* and related TBS policy and directive requirements relate to AAFC staff members' day to day job functions.

Management Response:

The CIO agrees with the recommendations to develop a needs and risks based privacy training strategy and modify privacy awareness training sessions.

Action Plan:

I. The ATIP Office will review its current privacy training strategy to determine how training can be delivered most effectively, with a view to target those branches/divisions who require immediate training based on need and risk.

II. The ATIP Office will review the current training material to ensure privacy awareness training is delivered effectively and content is relevant and practical for the range of day-to-day functions performed within AAFC. Updating content will be an ongoing process to remain current as changes occur.

Lead Responsible: CIO

Target Dates for Completion:

I. October 2010
II. March 2011

2.3 Third Party Delivery of Programs

Control and monitoring need improvement to ensure the appropriate management of personal information by third parties under contribution agreements or contracts.

The personal information collected and used by the majority of third parties is considered to be under the control of AAFC even if it is not provided to AAFC during the course of program administration and, therefore, AAFC is accountable in these cases to ensure it is managed in accordance with the *Privacy Act*[2].

Guidance has not been provided to program areas on how to ensure third party delivery agents appropriately manage personal information collected on behalf of AAFC. Although contribution agreement templates for third party delivery agents contain clauses addressing the necessary high-level privacy requirements, there is often little practical guidance from program areas provided to the delivery agents on how these requirements translate to program processes/procedures. For example, guidance is often not provided on the appropriate privacy notice required on program forms that may have been designed and are being utilized by the third party delivery agent (and co-branded with the AAFC logo).

In the absence of corporate guidance, established programs such as APP have developed their own third party processes which could be further enhanced in some respects.

[2] Guidance from TBS states that "*Personal information is considered to be under the control of a government institution when that institution is authorized to grant or deny access to it, to direct its use and, subject to the approval of the National Archivist, to dispose of it. Personal information which is in the possession or custody of an institution, whether at headquarters, regional, satellite or other office, either within or outside Canada, is presumed to be under its control unless there is strong evidence to the contrary*". AAFC has registered Personal Information Banks (PIBs) and Retention and Disposal Authorities (RDAs) for these programs, both actions indicating AAFC has de facto control of the personal information. Furthermore, the agreements with the delivery agents outline AAFC's right to access the information.

Each year, APP administrators must reapply to act as administrators for APP. While successful applicants are subject to the Advance Guarantee Agreement which includes an Appendix dictating privacy procedures, the application form for these administrators misses the opportunity to provide upfront an explanation of the administrators' required personal information management and privacy practices and applicants are not required to share their current practices with AAFC.

The privacy practices of third parties are currently not specifically monitored or audited, except when an incident or breach occurs. In 2008, there was a significant privacy breach related to the inappropriate privacy practices of a third party delivery agent. While the Centre of Program Excellence (COPE) Recipient Audit Unit (RAU) is now responsible for all recipient compliance audits within the Department, the current Recipient Risk Management Framework utilized by RAU does not specifically allow for consideration of the nature of the personal information collected and used or the privacy practices of third parties in the risk assessment of third party delivery agents. In addition, the Annex (to the template SOW for recipient audits) that provides the minimum audit criteria to assist the auditor in the design of the audit program to meet the audit objectives does not include privacy considerations that could be applied to audits of third party delivery agents.

Given the current lack of departmental guidance to program areas and ultimately to third parties, third parties may not be aware of their responsibilities related to the management of personal information and of how to apply these privacy requirements to the day to day administration of their programs.

Recommendation 3a

The Chief Information Officer should:

I. Issue clear guidelines on the responsibility of AAFC programs to ensure third parties comply with the requirements of the *Privacy Act.*
II. Develop guidance that can be provided to third parties by program managers on how to translate privacy requirements contained in the contribution agreements/contracts with AAFC into program processes.

Management Response:

While AAFC has done a lot of work to ensure that its third party delivery contracts contain the appropriate privacy obligations, CIO agrees with the two parts of Recommendation 3.

It may not be in every case that a third party must comply with the Privacy Act. AAFC must comply with the Privacy Act and will ensure that the third party acts in such a manner pursuant to the agreements so as to ensure that AAFC can meet AAFC’s obligations under the Privacy Act.

Prior to issuing guidelines and guidance, the ATIP Office must clearly define the role of the Privacy Act in third party delivery scenarios and the interplay between federal legislation and provincial/private sector legislation when AAFC is developing contracts with provinces and third parties.

Action Plan**:**

I. The ATIP Office will define the approach to the protection of personal information in third party scenarios and then issue guidelines to programs.
II. Once guidelines have been issued, the ATIP Office will develop guidance suitable for provision to third parties (where appropriate). In the interim, AAFC will continue to provide input to individual agreements through COPE and the Tiger Team process.

Lead Responsible: CIO

Target Dates for Completion:

I. March 2011
II. March 2011

Recommendation 3b

The ADM, Farm Financial Programs Branch should develop a risk-based approach to monitoring third party compliance with privacy requirements, including ensuring privacy considerations are included in COPE Recipient Audit Unit's risk framework for the selection of recipient audits of third party delivery agents and in the Statements of Work for the conduct of third party delivery agent recipient audits.

Management Response:

The ADM, Farm Financial Programs agrees with the recommendation and has taken a number of steps recently to strengthen monitoring of third party compliance with privacy requirements. A privacy project completed between November 2008 and March 31, 2009 resulted in, among other actions, new guidelines for APP administrators and FFPB having the capacity to audit and monitor third party compliance with privacy requirements.

Action Plan:

I. COPE Recipient Audit Unit will incorporate sufficient language, which has been reviewed and commented on by the AAFC ATIP Division, to address ATIP concerns within the AAFC Recipient Policy, the Escalation Process for Alleged Wrongful Disclosure, Fraud, Privacy Breach, or Misappropriation, the Overpayments Recovery Process for Dealing with Audit Adjustments, the Recipient Risk Management Framework (RRMF) and the Recipient Audit Statement of work (SOW).

Lead Responsible: ADM, FFPB

Target Date for Completion: March 2011

2.4 Use of the Social Insurance Number (SIN)

While AAFC has made significant strides in recent years in modifying its processes to ensure compliance with the TBS Directive on the Social Insurance Number (SIN), there remain a number of practices that are not consistent with the Directive.

The SIN is considered an especially sensitive data element that, if compromised, may lead to identity theft or other inappropriate activity. The Directive requires that the SIN only be collected and used for authorized purposes; in the case of AAFC, this generally only relates to programs that are providing a taxable benefit. The SIN can only be collected and used to report this taxable benefit to Canada Revenue Agency (CRA).

Current practices observed within AAFC that are not consistent with the spirit of the TBS SIN Directive include:

- FIPD utilizes the name, address, and SIN of producers to create a unique identifier (i.e. a producer PIN).
- The hardcopy files of producers at FIPD contain the producer's SIN on the outside of the folder.
- To obtain an activation code to access the My Account website, producers must provide their SIN (in addition to their PIN and postal code),
- As the PIN created by FIPD is not universally used throughout AAFC, the SIN is one of the data elements that has been exchanged between programs in order to match individual producers between programs. For example, this exchange has occurred between FIPD and the Agri-Environment Services Branch,
- AAFC programs such as the Hog Farm Transition Program (HFTP) are collecting the SIN from all applicants at the time of application, although the collection of the SIN from individuals that do not receive funding is not consistent with the TBS Directive, especially for a program such as HFTP, where slightly less than half of those registering for the program have not ultimately received funding from AAFC.

Recommendation 4a

The Chief Information Officer should develop AAFC guidelines, consistent with the requirements of the TBS Directive, on limiting the collection, use and retention of the SIN.

Management Response:

The CIO agrees with the recommendation

Action Plan:

I. ATIP will communicate TBS directives on the SIN and its appropriate use by AAFC-AAC

Lead Responsible: CIO

Target Date for Completion: December 2010

Recommendation 4b

The ADM, Farm Financial Programs Branch should ensure the SIN is removed in a timely manner from FFPB's processes, files and systems where it is no longer required (e.g. the hardcopy files within FIPD, producers who have not received funding under AAFC programming).

Management Response:

The ADM, Farm Financial Programs agrees that SINs should not be retained where they are no longer required.

Action Plan:

I. FIPD is no longer including the producers' SIN on the outside copy of hardcopy folders in the FIPD file room.
II. Hardcopy files that remain on-site will have the SIN on the outside of the folder blacked out.
III. Going forward with the new AgriStability and AgriInvest systems, in cases where clients have not filed for two years and have never received a payment, SINs will be removed.
IV. FIPD is ready for the archiving of databases for programs that have wound down. FIPD will further restrict access to databases for programs winding down.

Lead Responsible: ADM, FFPB

Target Dates for Completion:

I. Completed
II. March 2011
III. March 2013
IV. March 2011

2.5 AAFC Service Excellence Agenda

While PIAs have been performed on many of the separate components of the Service Excellence Agenda (Agenda), a PIA specific to the Agenda has not been completed.

PIAs must be conducted on initiatives involving personal information; the conduct of a PIA at an early stage ensures privacy requirements are appropriately considered during the requirements definition and development stage.

As part of the AAFC Service Excellence Agenda, which has a goal of bundling and integrating services, AAFC is continuing to work on a producer hub (i.e. a common producer database) intended to be utilized by all programs under the Agenda. Common tombstone data on an applicant will be available to all participating programs.

The bundling and integration of services through the Agenda is a significant undertaking that raises new privacy issues not only for the components that form the Agenda, but also for the Agenda as a whole.

Although specific privacy risks have yet to be identified for the Agenda, *Privacy Act* requirements that must be thoroughly considered during the development phase of the Agenda include:

- Personal information collected is directly related to a program or activity (and proper authority has been identified), collected directly from the data subject (with limited exceptions), and appropriate notice is provided.
- Personal information is only used and disclosed for a purpose consistent with its original collection, unless consent of the data subject is obtained or it is authorized under the *Privacy Act*.

AAFC has developed an initial Agenda-specific privacy framework to address privacy concerns and issues which may arise from the design and implementation. The framework indicates that PIAs have already been performed on many of the separate components that make up the Agenda and that any concerns identified are to be included in the Agenda PIA. It is important, however, in order to ensure all risks are appropriately identified and mitigated, that the Agenda PIA assesses the potential privacy impacts of the Agenda as a whole, and not just those of the individual components, as the interaction of these components raises additional privacy issues. For example, if the common producer database will be available to a number of programs; this data sharing could present a privacy risk if personal information in the common producer database has been collected for a specific purpose but is then used for inconsistent purposes by other programs, which would otherwise typically require the consent of the producer.

Recommendation 5:

The ADM, Farm Financial Programs Branch should ensure that a PIA is conducted at an early stage for the Service Excellence Agenda as a whole and be subsequently updated at key milestones throughout the design and implementation of the Agenda.

Management Response:

The ADM, Farm Financial Programs Branch agrees with the recommendation. A privacy analysis was conducted to determine the most effective approach to identifying and addressing privacy concerns. Based on the framework, it was determined the best method was to conduct two separate Privacy Impact Assessments (PIAs), a global and a generic.

Action Plan:

I. The Global PIA has been completed with the exception of the Grants and Contributions Delivery System (GCDS) component which will be completed by March 2011
II. The Generic PIA will include all non-Business Risk Management (BRM) Grants and Contributions Programs. FFPB and ATIP continue to work together and, where required, a plan to avoid or mitigate any adverse effects will be analyzed and added to the PIAs as the Service Excellence components continue to be developed.
.

Lead Responsible: ADM, FFPB

Target Dates for Completion:

I. March 2011
II. March 2011

2.6 Privacy Impact Assessments (PIAs)

While the ATIP Office has made significant progress in centralizing the PIA process to ensure all PIA activity is channeled through the ATIP Office, decisions to conduct a PIA or not have not been documented and there has been, as a result of the previous lack of resources and focus on PIAs at the ATIP Office, a backlog in their approval and a lack of follow-up to determine if risks have been appropriately mitigated.

PIAs must be conducted on initiatives involving personal information and the timely review of PIAs, and mitigation of identified risks, ensures program areas have implemented the appropriate privacy controls to protect personal information.

The decision to conduct or not conduct a PIA is not formally documented, as the ATIP Office has not been consulted by those program areas within the FFPB that have determined a PIA is not required.

There have been significant delays in some cases related to the review and approval of the PIAs from program areas reviewed (APP, FIPD AgriStability and AgriInvest) and from the HR Branch. In particular, the PIA conducted on FDMS as part of a PIA on Renewal Programs in 2006 has yet to be reviewed or approved by the ATIP Office.

Although action plans have been developed for those PIAs that have been reviewed by the ATIP Office, the Office or other departmental oversight bodies have not determined the extent to which the risks identified have been mitigated by the program areas.

The gaps related to the completion, assessment and follow-up of PIAs may result in privacy risks not being appropriately assessed, lack of compliance with policy requirements, and missed opportunities to learn and share lessons in terms of common risks/issues and most appropriate mitigation measures.

The ATIP Office has drafted a PIA Directive and associated procedures that outline the PIA process, including roles and responsibilities, but this has yet to be approved, and requires updating based on the new TBS Directive on PIAs.

Recommendation 6:

The Chief Information Officer should:

I. Finalize the AAFC PIA Directive and related procedures, ensuring the requirements of the new TBS PIA Directive are taken into account and that the responsibility is clearly assigned for following up on PIAs to determine if risks have been appropriately mitigated.
II. Focus on reducing the backlog of PIAs waiting for review and approval.

Management Response:

The CIO agrees with both parts of recommendation 6.

Action Plan:

I. A draft AAFC PIA Directive is in progress and will be updated as TBS communicates its final guidelines on the new PIA directive.
II. ATIP has devised an approach to expedite the backlog of PIAs for approval and continues to adjust as necessary.

Lead Responsible: CIO

Target Dates for Completion:

I. March 2011
II. March 2011

2.7 Retention of Personal Information in Electronic Format

Electronic information which may include personal information is generally not disposed of in accordance with defined Records Disposition Authority (RDA) schedules.

Personal information should only be retained for as long as it is necessary, and in compliance with approved RDAs.

Databases, such as the Net Income Stabilization Account (NISA) Client Services System (NCSS) utilized by FIPD and PeopleSoft utilized for HR functions, have retained electronic records past their disposition dates and personal information that is no longer required remains in FIPD, APP and FDMS program shared drives instead of being deleted.

The retention of personal information for longer than required for the purposes for which it was collected increases the risk of an unauthorized use or disclosure of personal information and may lead to a privacy breach.

Although the vetting of personal information becomes technically challenging for complex systems, it can be more quickly implemented for data stored on shared drives. The regular cleaning up of personal information on shared drives should be incorporated as part of program procedures.

Recommendation 7:

The Chief Information Officer should establish a formal plan to actively offer assistance to program areas in updating their disposition schedules and in ensuring that their electronic records are disposed of in accordance with those schedules.

Management Response:

The CIO agrees with this recommendation.

Action Plan:

I. ISB will provide the branches the existing retention and disposition schedule and will assist the branches with the disposition process.
II. ISB will schedule meetings with all branches to initiate discussions at the senior management level.
III. Repeat this process periodically.

Lead Responsible: CIO

Target Dates for Completion:

I. October 2010
II. January 2011
III. Ongoing