Office of the
Privacy Commissioner
of Canada

CANADA REVENUE AGENCY

**Audit Report of the
Privacy Commissioner of Canada**

Section 37 of the *Privacy Act*

FINAL REPORT

2013

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

613-947-1698, 1-800-282-1376
Fax 613-947-6850
TDD 613-992-9190
Follow us on Twitter: @PrivacyPrivee

Cat No. IP54-53/2013
ISBN 978-1-100-54620-9

This publication is also available on our website at **www.priv.gc.ca**.

Table of Contents

Main Points

WHAT WE EXAMINED

The Canada Revenue Agency (CRA or the Agency) administers tax laws and various benefit programs for the Government of Canada and several provinces and territories. This requires the collection and use of taxpayer information. We looked at how this information is managed, with a particular focus on how the Agency assigns and monitors access to taxpayer information by its employees.

Our audit examination was conducted between July 13, 2012 and March 31, 2013. During the audit we reviewed the way that the Agency assigns privacy responsibilities, manages privacy risks and ensures compliance with the *Privacy Act*. We examined the Agency's personal information management policies and procedures, training materials, privacy impact assessments, breach investigations, internal audits and security reviews. We also reviewed information technology security, access to electronic systems and the monitoring of employees who access taxpayer information on a daily basis. Finally, we interviewed numerous officials at the Agency's headquarters and in its four largest regions—Ontario, Pacific, Prairies and Quebec.

WHY THIS ISSUE IS IMPORTANT

The Agency collects income taxes and delivers benefits to more than 27 million Canadian taxpayers and has one of the largest personal information record holdings in Canada. In addition, taxpayer files contain highly sensitive financial, health, employment, family and identifying information.

Taxpayer information is the cornerstone of the administration of the CRA's tax related programs and services. The Agency is dependent on Canadians' personal information to collect taxes necessary to pay for public programs and services.

The CRA operates within a voluntary compliance regime when collecting taxes. More than 91 per cent of Canadians filed their income tax returns and 94 per cent paid amounts due on time last year. At the same time, taxpayers expect the Agency and its officials to be vigilant in ensuring that all necessary steps are taken to protect their personal information from inappropriate access, use or disclosure.

Over the past number of years our office has been informed about privacy breaches involving the inappropriate access to taxpayer information at the Agency. We were made aware of these breaches by Agency officials, complainants or through the media.

Privacy breaches could potentially have a serious impact on the individuals affected in the form of identity theft and fraud, financial hardship and/or personal embarrassment. Privacy breaches could also tarnish the Agency's reputation as a trusted custodian of Canadians' sensitive personal information.

WHAT WE FOUND

The CRA has a culture of security and confidentiality through its integrity framework, policies, training and awareness and other initiatives. Marked weaknesses exist however in the implementation and monitoring of some of its key privacy and security policies and practices. These weaknesses impair CRA's ability to ensure that taxpayer information is as secure as it can be from inappropriate internal access, use or disclosure. Most notably,

- Fulfilling a commitment stretching back to our 2009 audit, the CRA appointed a Chief Privacy Officer (CPO) on April 3, 2013. However, the role of the CPO has not been fully defined to ensure Agency-wide coordination of privacy accountabilities, responsibilities and activities.
- Privacy Impact Assessments are not always completed to assess risks prior to the implementation of program changes affecting taxpayers' personal information.
- Threat and Risk Assessments are not completed for many information technology systems that process taxpayer information which may result in undetected weaknesses.
- The effectiveness of the Agency's controls to detect and prevent inappropriate employee access and use of taxpayer information is limited by its lack of an automated tool to identify and flag potentially inappropriate accesses and by certain gaps in the collection of audit trail information for CRA computer systems.
- Inappropriate accesses to thousands of taxpayers' files have gone undetected over an extended period of time.
- The Access to Information and Privacy Directorate is not regularly informed about privacy breaches involving inappropriate access to and disclosure of taxpayer information.

Since our last audit report in 2009, the CRA has made progress to strengthen its privacy and security policies and procedures, and to communicate its expectations to employees about the safeguarding of personal information. Agency plans are also underway to improve access rights management and to more closely monitor employee access to taxpayer information.

The observations and recommendations in this report are intended to enhance the Agency's personal information handling practices—and by extension, mitigate the risk of unauthorized access, use or disclosure of taxpayers' personal information.

The Agency has responded to our audit findings and its management responses follow each report recommendation.

Introduction

ABOUT THE CANADA REVENUE AGENCY

The CRA administers tax laws and various social and economic benefit and incentive programs for the Government of Canada and for most provinces and territories.

The Minister of National Revenue is accountable to Parliament for all Agency activities, including administering and enforcing the *Income Tax Act*. The CRA Board of Management exercises corporate oversight on the Minister's behalf including strategic planning.

The Agency Commissioner appointed as Chief Executive Officer has the day-to-day responsibility for the administration of and compliance with various pieces of legislation including the *Income Tax Act* and the *Privacy Act*. The Commissioner and Assistant Commissioners sit on the Agency Management Committee, which provides policy direction, management control and risk management accountability across the Agency.

To fulfill its mandate as Canada's tax collector, the CRA has one of the most extensive personal information record holdings in Canada. In 2012 the Agency received almost 27 million individual tax returns, issued more than 34 million tax payments, sent 111 million credit and benefit payments to almost 12 million Canadians and responded to nearly 18 million public inquiries. The CRA interacts with more Canadians than any other government organization and its operations have a significant impact on individuals and businesses.

In 2012 the CRA had approximately 40 thousand employees working in five regions and 40 tax service offices and tax centres across Canada. Approximately 65 per cent—or 26,000—of CRA's employees have electronic access to taxpayer information through various tax systems.

The CRA is subject to the *Privacy Act* and associated Treasury Board policies and directives for the management and protection of Canadians' personal information. Section 241 of the *Income Tax Act* also imposes confidentiality requirements on its employees and others with access to taxpayer information. Penalties may be imposed if the Act is not respected.

Exhibit 1: Protection of Taxpayer Information under the *Income Tax Act*

241. (1) Except as authorized by this section, no official or other representative of a government entity shall

(a) knowingly provide, or knowingly allow to be provided, to any person any taxpayer information;

(b) knowingly allow any person to have access to any taxpayer information; or

(c) knowingly use any taxpayer information otherwise than in the course of the administration or enforcement of this Act, the *Canada Pension Plan*, the *Unemployment Insurance Act* or the *Employment Insurance Act* or for the purpose for which it was provided under this section.

Additional information about the Agency is available at www.cra-arc.gc.ca.

FOCUS OF THE AUDIT

The audit focused on employees' electronic access to taxpayer information. The audit objective was to determine whether the CRA has appropriate controls and safeguards in place to protect taxpayers' personal information, and whether its policies, processes, procedures and practices comply with the fair information practices as described in sections 4 through 8 of the *Privacy Act*.

The audit did not include an examination of personal information management practices related to the taxation of business clients, the Goods and Services Tax, the Harmonized Sales Tax or excise tax operations. The audit examination also excluded areas such as third-party access to individual taxpayer information, taxpayers' internet access to Agency services and the recent transfer of certain IT services to Shared Services Canada.

Observations and Recommendations

1. Our audit observations and recommendations are organized in four categories:

   - privacy management and accountability;
   - information technology security and governance;
   - employee access and monitoring; and
   - privacy breaches.

PRIVACY MANAGEMENT AND ACCOUNTABILITY

2. To meet the obligations of the *Privacy Act*, an organization must establish accountability for its compliance with the law. Our past audits of government institutions have shown that when accountability is not clearly defined, gaps exist in the coordination and implementation of privacy related responsibilities. Those accountability gaps can place personal information at risk.

3. The Minister of National Revenue is accountable for the CRA's administration of the *Privacy Act* and its compliance with Treasury Board's (TB) policy instruments. As the CRA's chief executive officer, the Commissioner is responsible for the day-to-day administration of the program legislation that falls under the Minister's delegated authority and for overall compliance with the *Privacy Act*.

4. The Access to Information and Privacy (ATIP) Director is responsible for much of the delivery of the Agency's multifaceted privacy program. The ATIP directorate responds to privacy requests and complaints; develops policies, procedures and training materials; reviews and provides advice on privacy impact assessments; and analyzes privacy breaches. The Director also chairs the ATIP Oversight Review Committee, which is a forum for branch directors to discuss and resolve privacy and access to information issues. The Director reports to the Assistant Commissioner Public Affairs who sits on the Agency Management Committee.

5. In recent years, the CRA has developed a comprehensive suite of privacy policies and related documents, including its Privacy Policy, Privacy Practices Directive, Procedures for Privacy Assessments, Privacy Breach Protocol, and Discipline Policy among others. Overall, the Agency's privacy management and accountability framework has a number of good features to ensure the protection of taxpayers' personal information.

Privacy Accountability needs to be defined

6. Considering the large volume and high sensitivity of taxpayer information held by the Agency, we expected to find that the CRA would have established strong privacy leadership under the position of a CPO to advance and monitor the CRA's privacy program and ensure compliance with the *Privacy Act*.

7. Many organizations in the public and private sectors have come to realize that strong privacy leadership at the top for the protection of clients' personal information is essential to maintaining their trust and goodwill. Client confidence is also a prerequisite for an organization to carry out its mandate and deliver its programs and services in an effective and efficient manner.

8. The appointment of a CPO by a federal government institution is not a requirement of the *Privacy Act*, nor is the role defined by Treasury Board policies[1]. Nevertheless, the appointment of such a senior privacy official has become increasingly a norm among many large organizations that manage extensive holdings of sensitive personal information. A CPO, appointed at the executive level of the organization, is responsible for overall strategic privacy direction and compliance of an organization.

9. The CPO is also responsible for ensuring that privacy impact assessments are conducted for new programs involving personal information. To fulfill these overlapping roles, the CPO is usually a member of the organization's senior management committee, where the CPO can speak authoritatively to colleagues on privacy matters; ensure that issues are understood; and solicit management support for organization-wide measures to reduce or mitigate privacy risks.

10. In 2009, the Agency committed to the naming of a Chief Privacy Officer and defining their role. Over the following three years, the Agency drafted a framework for the appointment of a CPO. However, the framework was not approved or implemented so no CPO was named over that period of time. Therefore, until quite recently the Agency did not have a privacy champion at its executive levels to promote the protection of personal information across the organization. Nevertheless, from 2009 to 2013, ATIP developed a number of key privacy policies and procedures and delivered diverse training initiatives.

11. On April 3, 2013, the CRA Commissioner notified Agency staff that a CPO had been appointed at the Assistant Commissioner level to ensure compliance with the *Privacy Act*, and to carry out other management, educational, risk assessment and reporting roles. This appointment was an important step in strengthening the Agency's privacy management regime. However, for the full benefit of the appointment of the CPO to be felt across the organization; the extent of the mandate, role and core activities of the official appointed needs to be formalized and defined more fully.

12. RECOMMENDATION

The Canada Revenue Agency should define fully the role of the Chief Privacy Officer and monitor the implementation of the CPO mandate in terms of employee privacy awareness, privacy risk reduction and overall Agency compliance with the *Privacy Act*.

Agency's response:

As noted in the report, the appointment of a Chief Privacy Officer (CPO) by a federal government institution is not a requirement of the Privacy Act, *and the role is not defined by Treasury Board policies.*

Nonetheless, the Canada Revenue Agency (CRA) agrees with this recommendation, and appointed a CPO to oversee privacy management in the Agency in April 2013. The CPO is a member of the Agency Management Committee (AMC) and has a broad mandate for privacy oversight in the Agency, including:

- *overseeing decisions related to privacy, including privacy impact assessments;*
- *championing personal privacy rights in accordance with legislation and policy, including management of internal privacy breaches—a shared responsibility with Security; and*
- *overseeing privacy awareness within the Agency through fulfillment of diverse communications and training activities.*

[1] Our Office has issued guidance to organizations about how to define the role of a CPO to meet their particular needs (*Getting Accountability Right with a Privacy Management Framework* 2012). While this document was intended for organizations subject to private sector privacy legislation, public sector institutions may also find it helpful.

The CPO, who is responsible for liaison with the Office of the Privacy Commissioner, will monitor and report on overall Agency compliance with the Privacy Act *by reporting to the Agency's senior management on the state of privacy management in the CRA at least twice each fiscal year.*

Employees understand their duty to protect taxpayer information

13. Compliance with the requirements and spirit of the *Privacy Act* depends largely on how well its requirements are understood by officials handling personal information in their employment duties. Employees must be educated on departmental privacy policies, procedures and guidelines, and should possess a clear understanding of their roles and responsibilities to protect clients' personal information.

14. We therefore expected to find that the CRA would have training and awareness measures in place to ensure that its employees fully understand their responsibilities to properly manage and protect taxpayers' information. We reviewed privacy, security and values and ethics training materials and other information resources available to employees on the Agency's intranet site. We also interviewed employees, and received briefings from officials responsible for coordinating privacy and security awareness training initiatives.

15. With close to 26,000 employees accessing taxpayer information on a daily basis, delivering ongoing privacy and information security training is a major task and it is for that reason that the CRA makes use of both formal and informal means to reach its employees.

16. We found that the CRA has invested considerable time and resources to develop comprehensive privacy and information security training plans. Privacy training involves face-to-face sessions and other awareness activities delivered through the Agency intranet, e-mail or meetings with employees. More than 5,600 CRA employees and managers have received direct privacy training since 2010. The Agency continues to make significant efforts to maintain and enhance privacy awareness.

17. Our interviews with CRA managers and supervisors confirmed that they had received privacy and security awareness training. These middle managers supervise large numbers of front-line employees. We also found that these officials had a sound understanding of their responsibility to ensure that they and their employees respect and safeguard personal information at all times.

Tools have been developed to assess privacy risks

18. Under the *Treasury Board Policy Framework for Management Risks*, Deputy Heads are responsible for managing their organization's risks by leading the implementation of effective risk management practices—both formal and informal.

19. Organizations use a range of tools to evaluate and manage privacy risks, including corporate risk assessments, internal audits, threat and risk assessments and privacy impact assessments. We expected that the Agency—depending on the circumstances—would use one or more of these tools to assess, limit and mitigate risks related to the management and protection of taxpayer information.

20. The CRA's Enterprise Risk Management Policy requires that a corporate risk plan be prepared to assess and report on a range of major operational and compliance risks across the Agency. The Agency takes an 'all-risks' approach to corporate risk management, which means it considers inherent as well as current risks.

21. The Chief Risk Officer at the CRA is an Assistant Commissioner and heads the Agency's corporate risk planning process. The same official has also recently taken on a complimentary role of Chief Audit Executive.

22. The Agency's corporate risk planning process includes a three year review of risks with an impact on the organization's mandate. The review gathers risk assessments from several major program areas and combines them into one Corporate Risk Assessment and Action Plan for the whole Agency. Annual surveys of corporate risks are also conducted to incorporate any new or evolving issues into the plan.

23. The Corporate Risk Profile identifies a strong interconnection between risks to the protection of personal information and risks related to employee ethical conduct. It also indicates that both of these risks have the potential to directly influence the Agency's reputation and public image. It is clear that if an Agency employee acts inappropriately with taxpayers' personal information, and this is made known publicly, the event may negatively affect the trust and confidence Canadians place in the Agency.

24. Internal audits and other reviews are other tools that have been used by the CRA to assess the management of employee access rights and the monitoring of employee use of personal information. These audits and studies have helped the Agency understand its current situation with regards to employee access. Based on this internal audit work, the CRA has been able to identify gaps in its controls, and develop a long term strategy to introduce new and enhanced measures to reduce privacy and security risks.

Privacy Impact Assessments are not always completed before projects are implemented

25. A Privacy Impact Assessment (PIA) is a tool used to evaluate potential privacy risks if a project, initiative or program change were implemented. A PIA then forecasts the probable impacts and harm to clients' personal information and the organization's reputation from the privacy risks identified. Finally, the PIA may be used by organizations to develop solutions to proactively prevent, limit or mitigate privacy risks to clients' personal information.

26. By design, a PIA provides valuable privacy risk analysis at an early stage of a project planning process. Completing a PIA prior to implementing a program or service reduces potential complications and costs which could result from its cancellation, delay or modification—if privacy risks are found after the fact. Integrating privacy protections into a project at the outset is generally much more effective and efficient than trying to fit them in afterwards.

27. The Treasury Board introduced a *PIA Policy* in 2002 to ensure privacy principles and protections are considered for all new or substantially redesigned programs and services in the federal public sector. The policy was replaced with the Directive on Privacy Impact Assessments in April 2010. For an organization to comply with the PIA Directive, mechanisms must be in place to identify and review new or revised activities that affect the management of personal information. To determine if a formal privacy risk assessment needs to be completed, organizations generally start with a preliminary assessment of privacy risks that a new or revised program may create.

Exhibit 2: When is a PIA required?

A PIA is generally required for a new or revised program if it:

- uses or will use personal information in a decision-making process that directly affects an individual;
- substantially modifies existing programs or activities where personal information is being used, or is intended to be used, in a decision-making process that directly affects an individual;
- contracts out or transfers a program or service to another level of government or the private sector resulting in substantial modifications to a program or activity;
- substantially redesigns a system or process that deliver a program to the public; or
- collects personal information, which will not be used in a decision-making process that directly affects an individual, but which will have an impact on privacy.

Government departments and agencies conduct PIAs. A PIA team within an organization often brings together experts from several areas, including programs areas, privacy, and access to information, legal services, and information technology. Once reviewed and approved by the organization, PIAs are sent to the Treasury Board Secretariat, and copies are also sent to the Office of the Privacy Commissioner for review.

Source: Based on Treasury Board Directive on Privacy Impact Assessments, April 2010.

28. We therefore expected that the CRA would have established a framework to evaluate privacy risks associated with new or substantially modified programs or systems. We also expected to find that PIAs would be completed before any such new or modified project or program is implemented.

29. In 2012, the CRA implemented comprehensive procedures and templates for conducting PIAs. These instructions define roles and responsibilities in the process, and provide a step-by-step approach for the preparation, review and approval of PIAs. The CRA has also developed a PIA questionnaire which allows the responsible program area and the ATIP Directorate to review information about possible privacy risks and to determine if a PIA is required.

30. Five PIA files were selected for examination from a CRA 2012 list of PIAs. Each file reviewed was either in the preparation, review or approval stages. From our examination, we found that although two years or more had elapsed since the projects were implemented, necessary PIAs had not been completed. Nor did we find any information on these files to indicate when or if a PIA would be completed.

31. If privacy risks are not adequately assessed before new or revised programs are implemented, the Agency may be unable to determine their potential impact on taxpayers and come up with solutions to prevent risks and to reduce and mitigate harm. In addition, it is not possible in such circumstances for our office to play our role in the PIA process as defined by the Directive on PIAs to: review, analyze and provide guidance on new and revised initiatives and programs.

32. RECOMMENDATION

Consistent with the Treasury Board Directive on Privacy Impact Assessments, the Canada Revenue Agency should complete, review and approve Privacy Impact Assessments prior to the implementation of any new program or initiative that may raise privacy risks to taxpayer information.

Agency's response:

The CRA agrees with this recommendation. The CRA will ensure that privacy impact assessments (PIAs) are completed, reviewed, and approved prior to the implementation of any new program or initiative that may raise privacy risks to taxpayer information.

To fulfill this obligation, the Chief Privacy Officer has been given overall responsibility for reviewing the status of PIAs in accordance with the CPO mandate. Accountability for completion of PIAs by senior officials in the organization will be monitored on a regular basis by the CPO and reported to the Commissioner and senior management.

INFORMATION TECHNOLOGY SECURITY AND GOVERNANCE

33. Information security is best achieved when it is supported by all levels of an organization, when it becomes an integral component of strategic and operational planning, and when it is embedded into the organization's practices, culture, day-to-day operations and employee behavior.

34. Sound information security practices are an essential component for meeting the requirements of the *Privacy Act* to protect Canadians' personal information. Organizations must implement appropriate controls to ensure personal information is not subject to unauthorized access, use, disclosure, alteration or destruction.

35. Treasury Board's *Policy on Government Security* establishes mandatory minimum security requirements for federal government organizations to protect and preserve the confidentiality and integrity of government assets including personal information. The Treasury Board *Operational Security Standard for the Management of IT Security* (MITS) and other security policies and standards, set out the framework of rules for organizations to follow for the safeguarding of their employees and their assets—including personal information.

Responsibility for IT security is clear

36. The Policy on Government Security states that federal departments and agencies must conduct risk assessments to determine whether their safeguards to protect their assets must be above mandatory minimum levels.

37. In November 2011, CRA transferred certain IT infrastructure functions to Shared Services Canada (SSC). Despite this transfer of functions to SSC, the Agency remains accountable for ensuring the protection of its personal information holdings related to its IT infrastructure.

38. We expected to find that the CRA would have a robust IT security governance framework and that accountability and responsibility under the framework would be clearly communicated to and understood by employees. We reviewed policies, plans, reports, project documentation, committee terms of reference and minutes, and conducted interviews with Agency management and staff.

39. Overall, the Agency Security Officer at the CRA has the responsibility for all aspects of CRAs security, including the security of taxpayer information. An Agency Security Plan identifies key security risks along with the strategies and plans for addressing them. These security documents are aligned with the overall corporate risk management process, which includes the identification, management and safeguarding of personal information and other information technology assets.

40. The Agency has established an executive-level committee with representation from relevant stakeholders which oversees all aspects of Agency security, including the security of its information. In addition, a joint senior management committee meets regularly to review and provide guidance on strategic and operational security initiatives.

Threat and risk assessments are not completed for many systems

41. The Treasury Board *Operational Security Standard on the Management of Information Technology Security* (MITS) mandates federal departments and agencies to certify and accredit their IT applications and systems before approving them for implementation. Without proper Certification and Accreditation (C&A), a system may operate without meeting government security standards and may also pose unintended privacy risks to the personal information it contains.

42. The purpose of certification is to verify that the security requirements established for a particular IT system or service are met and that the controls and safeguards work as intended. Accreditation means that management has authorized the system or service to operate and has accepted the residual risks based on the certification evidence.

43. According to MITS, a Threat and Risk Assessment (TRA) aids in the determination of security requirements. Organizations must apply security measures above minimum standards when justified by a TRA.

44. The *CRA Information Technology Threat and Risk Assessment Policy* states that all new systems and network applications should undergo the TRA process when being developed. We expected to find that the Agency's IT infrastructure would have been subjected to regular and ongoing security risk assessments to ensure that threats and vulnerabilities are identified and mitigated.

45. All CRA system platforms are currently undergoing a Harmonized Threat and Risk Assessment process. However, the Agency has identified many taxpayer applications that have not undergone adequate security assessments and where TRA and C&A processes have not been completed.

46. We found that the Agency has been piloting a C&A process[2]. This includes the introduction of a tracking and verification instrument to ensure that recommended actions identified through risk assessments are implemented. However, our review of key C&A documents for these projects demonstrated that follow-up was sometimes lacking to ensure that all steps in the process were completed and that recommended improvements were implemented. We did note however, that the Agency has recently instituted a process that includes a three-month follow-up on TRA recommendations for new applications.

[2] The CRA uses the term 'Security Assessment and Authorization (SA&A)' for their Certification and Accreditation process.

47. RECOMMENDATIONS

The Canada Revenue Agency should implement a Certification and Accreditation process that clearly assigns accountability and responsibility for the management of the process, as well as oversight to ensure C&A documentation is approved on time.

The Canada Revenue Agency should also prioritize critical systems and all related applications to ensure they undergo the Certification and Accreditation process and Threat and Risk Assessments.

Agency's response:

The CRA agrees with the recommendations. The CRA has a security evaluation process in place and continues to enhance this process based on evolving Treasury Board standards. The existing C&A processes will be enhanced to ensure security evaluations for all Agency applications as follows:

- *For future enterprise applications, the launch of a revised Security Assessment and Authorization (SAA) process which is consistent with the Treasury Board standard will ensure that newly developed applications will undergo complete C&A activities. It will be implemented by March 2014.*
- *For existing enterprise applications, CRA conducts an Annual Status Update of all security evaluations that were completed since 2008. A review of all existing applications is underway and outstanding security evaluations are being prioritized and addressed. Timeframes to complete the outstanding security evaluations, for applications identified as high priority, will be in place by March 2014.*
- *For local applications, a Local Application Repository (LAR) web application is in place to ensure that proper security evaluations are completed and tracked in accordance with the enhanced governance process described in our response to the recommendation at paragraph 55 below.*

Local applications are often implemented without review and approval

48. A local application is computer software used to respond to a local or regional administrative need or problem.

49. Important concerns about existing controls for local applications were raised in a CRA internal audit in 2007. At that time, the existing local application policy and related procedures were not always being followed by application owners. The registration of local applications in a Local Application Repository ('repository') and the recording of critical information about the applications were not being kept up to date in this central location. In addition, some local applications had been implemented before their mandatory review or approval.

50. In 2010 the CRA conducted a follow-up to its 2007 audit. Subsequently, the Agency instructed regional officials to register all local applications in the repository. This central record registry was meant to include an up-to-date list of local applications and record important details about their review, recommendations made, and approval by delegated Agency officials.

51. For our audit, we expected to find that the Agency would have fully implemented policies and procedures to manage local applications as recommended in its 2007 and 2010 audits. We found that Agency officials interviewed were familiar with and understood policies on local applications and that progress has been made since 2010 to strengthen its management of local applications.

52. However, we also found continued problems with the management of the repository and compliance with the Agency's local applications policies and procedures. Although some recent efforts have been made to rectify this situation in one of the offices we visited, we noted the repository is generally not being kept up to date; it contains old contact information; incorrect status notations and a number of local applications used in various regions are not listed.

53. We also observed a significant backlog for the review and approval of local applications. We reviewed 11 local application files and found that 9 used personal information; of these, 8 were still awaiting approval two to four years after their implementation and mandatory security and quality checks were not completed.

54. Without these security reviews and approvals being completed during the development of a local solution; the implementation of the application could result in an inadvertent breach of taxpayer information. The CRA informed us that Agency branches are now prioritizing the registration and security checks for local applications to reduce the existing backlog.

55. RECOMMENDATIONS

The Canada Revenue Agency should:

- Ensure that its policies, practices and procedures are followed to manage local applications and adequate safeguards are used to protect the taxpayer information they contain;
- Ensure that its Local Application Repository is reviewed regularly for completeness, accuracy and currency; and
- Follow up at each stage of the review and quality assurance processes and ensure that all local applications are approved by delegated officials before implementation.

Agency's response:

The CRA agrees with the recommendations. A review of the existing procedures and safeguards coupled with a current state assessment of the Local Application Repository (LAR) is targeted for completion by the end of July 2013. There will be an action plan in place by the end of September 2013 to address any gaps.

The governance process will be enhanced to include a mandatory review and approval process focusing on confirmation that privacy impact assessments and technical security reviews are completed prior to deployment in order to ensure completeness, accuracy, and currency. By the end of September 2013 all local application owners will be notified of the enhanced governance oversight.

EMPLOYEE ACCESS AND MONITORING

56. Organizations design and implement employee access and monitoring controls to prevent, limit, and detect unauthorized access to clients' sensitive personal information. Internal access controls include, among other things: password protections; user identification and authentication; and monitoring of user activity. Collectively, these controls when operating as intended can limit the possibilities of employees inappropriately accessing, using or disclosing personal information.

57. Our audit focused on internal controls to manage employee access rights, as well as the monitoring of employees' electronic access to taxpayer information.

Controls over access rights are being strengthened

58. *The Treasury Board standard on the Management of Information Technology Security* (MITS) notes that proper electronic access provisioning and removal is integral to ensuring information is accessed on a need-to-know basis. In particular:

- individuals must be security screened before being given access;
- access must be kept to a minimum required by individuals to perform their duties;
- access rights must be reviewed regularly to ensure that they accurately reflect the current responsibilities and employment status of the individual;
- access privileges must be removed for individuals who leave the organization, or are absent for a significant period of time; and
- access privileges must be modified when individuals move to jobs that do not require the same level of access.

59. We expected to find that the CRA would have processes and procedures in place to grant, remove and manage employee access to the CRA systems that process taxpayer information. We reviewed the Agency's process and procedures used to determine each employee's access level and privileges, and to update such privileges when an employee changes functions or leaves the organization.

60. We found that the Agency has an *Access Control Policy* and uses a standard Employee System Access Review (ESAR) process to establish and maintain employee access privileges. Such IT privileges are assigned to each employee based on their specific job functions, which may change depending on workload and other factors. Access privileges are reviewed at least twice yearly by managers using the ESAR process and other related tools. Access privileges are also verified and modified by managers as necessary when employees change job functions.

61. Our interviews found that managers and team leaders responsible for the review and approval of employees' access privileges were familiar with the ESAR process and found it to be an effective access management tool. Some suggestions were made about simplifying the process and increasing connectivity between ESAR and human resource information systems. This linking of employee information would potentially assist the verification of employment status and facilitate the updating of employees' access privileges.

62. The Agency is currently implementing a multi-phased and multi-year identity and access management project to improve controls and processes used to attribute, modify and remove employee access privileges. The CRA expects to further automate and strengthen the current access review process over the coming years.

63. RECOMMENDATION

The Canada Revenue Agency should continue to enhance its Identity and Access Management System controls to ensure that employee access is limited to only that information required to carry out their job functions, based on the need-to-know principle.

Agency's response:

The CRA agrees with the recommendation and will leverage the work that has been completed to date through the Identity and Access Management project, which includes the creation of the information resources completed March 2012, and the authoritative identity store implemented May 2013, and will:

- *continue to advance work already underway to review the roles and profiles used by managers to provision their employees which will be completed by October 2014;*

- *implement an enhanced annual verification process which will be completed by December 2014;*
- *continue implementing the remaining stages of the Identity and Access Management project and program.*

To date the CRA has invested approximately $10.5M and is planning a further significant investment to tackle this issue through both the Identity and Access Management as well as the Modernization of the National Audit Trail System projects.

Generic user IDs are not adequately controlled

64. Access controls for the identification and authentication of system users are very important tools because many other safeguards rely upon them. The MITS standard requires all federal government organizations to implement identification and authentication safeguards for all networks and systems. Controls implemented should be commensurate with the organization's level of inherent network or system risk. Organizations must also ensure that the identity of employees has been confirmed before assigning them a unique system user ID.

65. A generic user ID (Generic ID) is one shared by several users. Generic IDs are used for system processes and shared access to certain functions. They are also used by IT staff for system development, testing, and maintenance purposes. The use of Generic IDs allows more than one IT employee to verify system functionality without having to grant additional access to their personal user IDs.

66. However Generic IDs pose accountability and privacy risks. When Generic IDs are used, it makes it difficult for organizations to verify who accessed a system. While Generic IDs are logged when a system is accessed, the access cannot be readily attributed to a particular employee. Although generic IDs are often used in non-operational[3] test environments, these environments can contain sensitive taxpayer data.

67. We expected to find that the CRA would have implemented controls to manage and limit employees' use of Generic IDs. The Agency's user identification standard requires user IDs to be linked to a unique individual. The CRA has established a *Generic Account Administration Standard* and related procedures to manage exception cases when generic IDs are required to support operational needs.

68. We reviewed the use of Generic IDs within the Agency and found that they are subject to limited oversight. We also found that the Agency has an inventory of more than 10,000 such IDs, but it is not always clear from its records if they are in use, by whom and for what purposes.

69. CRA policy requires that Generic IDs be authorized by management and approved by the Information Technology Branch before use. However we found that they are not tracked centrally and there are many older Generic IDs which have not been approved. The CRA confirmed that reports produced on Generic IDs are not being reviewed to manage the use of these IDs.

[3] Non-operational test environments are used by IT Staff to develop and test systems before they are used to process tax returns in the regular business or operational environment.

70. RECOMMENDATIONS

The Canada Revenue Agency should review existing generic user IDs to determine whether they are required, authorized and controlled; and should delete all IDs that are not in use.

The Canada Revenue Agency should also ensure that all generic user IDs are subject to established review and approval processes.

Agency's response:

The CRA agrees with the recommendations and will:

- *strengthen the current process to introduce enhanced controls which will significantly reduce the number of generic accounts created which will be completed by December 2013;*
- *leverage the authoritative identity store already implemented in May 2013 to conduct a full review of all existing generic accounts and take necessary action including the deletion of those not in use and the assigning of accountability for each account to named individuals which will be completed by March 2014;*
- *enhance the security awareness and accountability surrounding generic accounts which will be completed by December 2014.*

Gaps exist in the monitoring of employee access to taxpayer information

71. To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is necessary to determine what, when, and by whom specific actions have been taken on IT systems. Organizations do this by using software that creates an audit trail—a log or record of an employee's actions on a system.

72. We expected to find that the CRA would have policies and procedures concerning audit logging and the review of such logs. Audit logging should be enabled on all systems that allow employee access to taxpayer information. Audit logs should also be subject to ongoing monitoring and timely notification of potentially inappropriate accesses. We reviewed CRA's procedures to monitor employee access and assessed the implementation of the monitoring process.

73. The Agency has developed a *Logging and Monitoring of Access to Taxpayer Information Policy*. The CRA logging policy requires that all employee access to its systems must be recorded—subject to limited exceptions. The CRA has tools to track and monitor employee access to taxpayer information on the majority of its systems.

74. The CRA's National Audit Trail System (NATS) has two components:

- Online Audit Trail System (OATS) is the Agency's primary monitoring tool that enables delegated managers to conduct random spot-checks of employee access to taxpayer information for a period of one to seven days. Any results that identify potentially inappropriate accesses are referred to the Internal Affairs and Security and Directorate (SIAD) division for further investigation.
- Audit Trail System (ATS) records historical data. An audit trail report may be requested by managers in response to a taxpayer complaint, in support of an investigation into alleged or suspected unauthorized access, or to respond to an access to information or privacy request. Access to ATS information is controlled by the SIAD.

75. In 2010, the CRA conducted audits to examine whether system audit trails were recorded, managed and monitored in accordance with Agency policy. These internal audits found that the CRA's logging policy did not provide enough guidance to managers on the use of audit trails as tools to monitor their employees' access; and identified a gap in system controls to follow up on, monitor or report the results of OATS reviews across the CRA.

76. The Logging Policy requires managers and team leaders to regularly conduct OATS reviews for all employees under their supervision. The purpose of these reviews is to detect employee accesses that are unusual or may be inappropriate, and in such instances to provide leads for further investigation.

77. We found that managers at the offices visited do not carry out their OATS reviews in a consistent manner. Few of the individuals interviewed had received formal training on how to conduct reviews. Many found the process to be complex, time consuming and largely ineffective. While the OATS process may serve to deter employees from inappropriately accessing taxpayer information, it was rarely perceived by managers interviewed as the primary source for detecting it.

78. We also found that the effectiveness of the Agency's controls to detect and deter inappropriate access and use of taxpayer information is limited by its lack of an automated tool to identify and flag potentially inappropriate employee accesses.

79. While Agency policy requires that all access to taxpayer information be logged, we found that some of the CRA's applications do not generate audit trail information.

80. The Agency briefed us on its plans to enhance the functionality of the current OATS monitoring system, and more effectively flag unusual or high-risk employee accesses for managers in its new audit log reports. The CRA is also considering options to strengthen the audit trail system through continual and proactive monitoring of employee actions.

81. RECOMMENDATION

The Canada Revenue Agency should continue to strengthen its audit logging system and process and the Agency should incorporate risk assessment tools to flag potentially inappropriate employee activities on its systems.

Agency's response:

The CRA agrees with the recommendation and will continue to strengthen its audit logging system and process capability by:

- *completing the implementation of the new Audit Trail Record Analysis Tool to assist management with the review of employee accesses which will be completed by December 2013;*
- *furthering the ongoing work to enhance technological tools and associated business processes to proactively analyze user transactions, provide for early identification of issues, and detect certain patterns of behaviour.*

As noted in recommendation at paragraph 63 (of the report), to date the CRA has invested approximately $10.5M and is planning a further significant investment to tackle this issue through both: the Identity and Access Management as well as the Modernization of the National Audit Trail System projects.

Access to taxpayer information by IT developers is inadequately monitored

82. Taxpayer information is copied into non-operational test environments (see footnote 3) as part of the development, testing, and maintenance of the Agency's IT systems. For example, the CRA downloads a subset of taxpayer information each year. This process enables IT staff to develop and test system modifications required for the next tax cycle without affecting the CRA's ongoing tax operations.

83. Certain IT development team members are granted read-only access to taxpayer information in operational environments. This type of access is approved to enable development staff to resolve problems with specific tax files. We expected to find that the CRA's general policies and procedures governing access to taxpayer information would also apply to IT developers.

84. Developers' access to systems and data in both test and operational environments is controlled using profiles that are assigned based on job requirements and the need-to-know principle. Access rights are reviewed semi-annually for these users through the standard ESAR process.

85. Audit trails in test environments record IT employees' access to taxpayer information. However, these audit trails are only retained for five days which hinders the Agency's ability to conduct follow-up on such accesses. In addition, audit trails generated from test environments are not incorporated into the Agency's National Audit Trail System.

86. Selected members of development teams also have the ability to transfer taxpayer information from operational to test environments. While there is a record of which user downloaded the information, there is no record indicating the specific taxpayer accounts downloaded.

87. RECOMMENDATIONS

The Canada Revenue Agency should ensure that adequate measures are in place to mitigate the risks associated with developer access to taxpayer information in test environments.

The Canada Revenue Agency should also rigorously control, track and monitor transfers of taxpayer information from operational to test environments.

Agency's response:

The CRA agrees with the recommendations. The CRA will increase the control environment specifically around the use of taxpayer data in test environments by:

- *updating and communicating its policy suite concerning populating and accessing taxpayer data in test environments. This will be concluded by March 2014;*
- *developing an options analysis which will identify the most effective method to control, track and monitor transfers of taxpayer information from operational to test environments. This options analysis will be completed by March 2014, with implementation of the approved option immediately following.*

PRIVACY BREACHES

88. The Treasury Board *Guidelines for Privacy Breaches* define privacy breaches as follows.

> "A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information… A breach may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders."

89. The Guidelines suggest that government organizations establish a plan for addressing privacy breaches that includes the following elements: preventing risks; limiting and mitigating the impact of breaches; conducting root cause analysis of the reasons for the occurrence; and implementing corrective measures to avoid similar problems in the future.

Exhibit 3: How to Respond to a Privacy Breach

Offices of Primary Interest

1. Take immediate action to stop the breach and to secure the affected records, systems or web sites.
2. Document the privacy breach.
3. Notify both the departmental Access to Information and Privacy (ATIP) Coordinator and the Departmental Security Officer as most privacy breaches involve a breach of security.

Departmental Security Officers and ATIP Coordinators

4. Depending on the process established at the institution, either the ATIP coordinator or the official responsible for security should notify the Deputy Head and the Communications Branch.
5. Conduct an internal investigation and make recommendations to prevent recurrence.

ATIP Coordinators

6. Notify the Office of the Privacy Commissioner... Notification should occur as soon as possible after the institution becomes aware of the breach (within days).
7. Notify individuals whose personal information has been wrongfully disclosed, stolen or lost... Notification should occur as soon as possible following the breach to allow individuals to take actions to protect themselves against or mitigate the damage from identity theft or other possible harm.
8. Follow up.

Source: Treasury Board Guidelines for Privacy Breaches, August 8, 2012.

90. We expected to find that the CRA would have a process in place to meet Treasury Board's expectations. Consistent with our recommendation from our 2009 audit of Privacy Management Frameworks, we also expected to find that the CRA would have implemented an information sharing arrangement for privacy breaches between the Security and Internal Affairs Directorate (SIAD) and the Access to Information and Privacy Directorate (ATIP).

Mechanisms to investigate privacy breaches are in place

91. From our review of files, we found that SIAD conducts thorough investigations of breaches when they occur. Our interviews with managers and team leaders confirmed that these officials were aware of what a privacy breach is, how and to whom to report such matters, and what role they are to play in the breach reporting and investigation processes.

92. In response to our 2009 audit recommendation, the CRA developed an *Agreement on Information-Sharing Protocol for Internal Privacy Breaches* (protocol) in April 2010. The protocol describes the roles of the Security and ATIP sections in the breach process.

ATIP is not regularly informed when a privacy breach occurs

93. The Treasury Board *Guidelines for Privacy Breaches* (TB guidelines) provides guidance to departments and agencies about the reporting and follow-up to privacy breaches:

> "It is important to involve the ATIP Coordinator and the Departmental Security Officer (DSO) to ensure that the privacy of individuals and the security of assets are taken into account in the resolution process. The departmental ATIP office should also conduct an assessment to uncover any deficiency in personal information management practices. This assessment and related recommendations should focus on issues that are not strictly linked to security issues. "

94. The CRA's Breach Protocol stipulates that when internal breaches involve personal information and will likely pose a risk of injury to any individual, the SIAD will inform the ATIP Director according to a risk assessment. However, the protocol does not require SIAD to report all privacy breaches to ATIP.

95. From our review of breach files and lists of breach investigations provided by the Agency, we found that SIAD does not regularly inform ATIP about privacy breaches. When ATIP is not kept informed of privacy breaches, it is unable to fulfill its role in reporting, analyzing and following-up on privacy breaches.

96. Our own records show that our Office is not regularly informed by the Agency about breaches involving employees' unauthorized accesses to and disclosure of taxpayer information. In addition, CRA breach files do not record the reasons why the Agency has decided not to notify affected taxpayers and our Office about privacy breaches. However, CRA has recently introduced a risk assessment process that includes the recording of reasons why the affected taxpayer and our Office should or should not be advised.

Serious breaches involving the disclosure of taxpayer information have occurred at the Agency

97. From a list of internal investigations conducted by the CRA during 2011 and 2012, we identified more than 50 that involved inappropriate access to taxpayer information. Our review of a sample of those investigations indicated that many also involved inappropriate disclosure of taxpayer information. Some files involved employee access to thousands of taxpayer files over an extended period of time during which they went undetected.

98. The Agency's records about access and disclosure breaches indicate that employee motivation varied from curiosity, to personal gain, preferential treatment and fraud. Where employee wrongdoing was established disciplinary measures were applied, ranging from a warning to dismissal.

99. RECOMMENDATION

Consistent with Treasury Board Guidelines for Privacy Breaches, the Canada Revenue Agency should ensure that the Access to Information and Privacy Directorate is notified of all breaches as they are discovered.

Agency's response:

The CRA agrees with this recommendation and continues to enhance its established information-sharing protocol by:

- *immediately expanding the existing protocol to include the notification of all breaches in accordance with the Treasury Board Secretariat Guidelines on Privacy Breaches;*
- *ensuring more timely breach notifications to the Access to Information and Privacy Directorate (ATIP).*

Conclusion

100. The *Privacy Act* imposes obligations on federal government institutions to respect the privacy rights of Canadians.

101. The CRA has a culture of security and confidentiality through its integrity framework, policies, training and awareness and other initiatives. Marked weaknesses exist however in the implementation and monitoring of some of its key privacy and security policies and practices. These weaknesses impair CRA's ability to ensure that taxpayer information is as secure as it can be from inappropriate internal access, use or disclosure. Most notably,

- Fulfilling a commitment stretching back to our 2009 audit, the CRA appointed a Chief Privacy Officer (CPO) on April 3, 2013. However, the role of the CPO has not been fully defined to ensure Agency-wide coordination of privacy accountabilities, responsibilities and activities.
- Privacy Impact Assessments are not always completed to assess risks prior to the implementation of program changes affecting taxpayers' personal information.
- Threat and Risk Assessments are not completed for many information technology systems that process taxpayer information which may result in undetected weaknesses.
- The effectiveness of the Agency's controls to detect and prevent inappropriate employee access and use of taxpayer information is limited by its lack of an automated tool to identify and flag potentially inappropriate accesses and by certain gaps in the collection of audit trail information for CRA computer systems.
- Inappropriate accesses to thousands of taxpayers' files have gone undetected over an extended period of time.
- The Access to Information and Privacy Directorate is not regularly informed about privacy breaches involving inappropriate access to and disclosure of taxpayer information.

102. Since our last audit report in 2009, the CRA has made progress to strengthen its privacy and security policies and procedures, and to communicate its expectations to employees about the safeguarding of personal information. Agency plans are also underway to improve access rights management and to more closely monitor employee use of taxpayer information.

103. The observations and recommendations in this report are intended to enhance the Agency's personal information handling practices—and by extension, mitigate the risk of unauthorized access, use or disclosure of taxpayers' personal information.

About the Audit

AUTHORITY

Section 37 of the *Privacy Act* empowers the Privacy Commissioner to examine the personal information handling practices of federal government organizations.

OBJECTIVE

The audit objective was to assess whether the Canada Revenue Agency has implemented adequate controls to protect taxpayers' personal information, and whether its policies, procedures and processes for managing such information comply with the fair information practices embodied in sections four through eight of the *Privacy Act*.

CRITERIA

Audit criteria were derived from the *Privacy Act* and Treasury Board Secretariat policies, directives and standards related to the management of personal information.

We expected to find that the CRA has:

- appropriate safeguards in place to protect personal information under its control;
- established clear accountability for privacy within the organization;
- a compliance mechanism to ensure that its obligations under the *Privacy Act* are met;
- a framework to ensure that privacy risks associated with systems, programs and activities are identified and mitigated;
- developed and implemented a privacy breach reporting and resolution mechanism;
- ensured that employees are aware of their responsibility and obligation to respect the privacy rights of taxpayers; and
- implemented the recommendations made in the Privacy Commissioner's 2009 report on Privacy Management Frameworks in Selected Federal Institutions.

SCOPE AND APPROACH

The audit examined the accountability and risk management frameworks, policies, procedures, processes, systems, administrative controls and technical safeguards governing employee access to and use of Canadian taxpayers' personal information.

The audit did not include a review of personal information related to the taxation of business clients, the Goods and Services Tax, the Harmonized Sales Tax, and excise tax operations. Nor did it look at third-party access to taxpayer information, web-based applications, or the transfer of certain IT services to Shared Services Canada.

The audit examined the CRA's practices and procedures to manage and protect taxpayers' personal information. During the audit, evidence was obtained from the examination of records, interviews with 101 officials, demonstrations of systems and other audit tests. Examination activities were conducted at the Agency's headquarters in Ottawa and at the regional tax centres in Shawinigan (Quebec), Sudbury (Ontario), Surrey (Pacific) and Winnipeg (Prairies).

The audit commenced on July 13, 2012 and was substantially completed on March 31, 2013.

STANDARDS

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner of Canada, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

AUDIT TEAM

Audit oversight:
Assistant Commissioner, Chantal Bernier

Auditors:
Tom Fitzpatrick
Gaétan Létourneau
Anne Overton
Rick Smith
Bryony Townsend
Matt Williams

Appendix A: List of Recommendations

Privacy Management and Accountability	
RECOMMENDATION	**AGENCY'S RESPONSE**
The Canada Revenue Agency should define fully the role of the Chief Privacy Officer and monitor the implementation of the CPO mandate in terms of employee privacy awareness, privacy risk reduction and overall Agency compliance with the ***Privacy Act***.	As noted in the report, the appointment of a Chief Privacy Officer (CPO) by a federal government institution is not a requirement of the ***Privacy Act***, and the role is not defined by Treasury Board policies. Nonetheless, the Canada Revenue Agency (CRA) agrees with this recommendation, and appointed a CPO to oversee privacy management in the Agency in April 2013. The CPO is a member of the Agency Management Committee (AMC) and has a broad mandate for privacy oversight in the Agency, including: • overseeing decisions related to privacy, including privacy impact assessments; • championing personal privacy rights in accordance with legislation and policy, including management of internal privacy breaches—a shared responsibility with Security; and • overseeing privacy awareness within the Agency through fulfillment of diverse communications and training activities. The CPO, who is responsible for liaison with the Office of the Privacy Commissioner, will monitor and report on overall Agency compliance with the ***Privacy Act*** by reporting to the Agency's senior management on the state of privacy management in the CRA at least twice each fiscal year.
Consistent with the Treasury Board Directive on Privacy Impact Assessments, the Canada Revenue Agency should complete, review and approve Privacy Impact Assessments prior to the implementation of any new program or initiative that may raise privacy risks to taxpayer information.	The CRA agrees with this recommendation. The CRA will ensure that privacy impact assessments (PIAs) are completed, reviewed, and approved prior to the implementation of any new program or initiative that may raise privacy risks to taxpayer information. To fulfill this obligation, the Chief Privacy Officer has been given overall responsibility for reviewing the status of PIAs in accordance with the CPO mandate. Accountability for completion of PIAs by senior officials in the organization will be monitored on a regular basis by the CPO and reported to the Commissioner and senior management.

Information Technology Security	
RECOMMENDATION	**AGENCY'S RESPONSE**
The Canada Revenue Agency should implement a Certification and Accreditation process that clearly assigns accountability and responsibility for the management of the process, as well as oversight to ensure C&A documentation is approved on time. The Canada Revenue Agency should also prioritize critical systems and all related applications to ensure they undergo the Certification and Accreditation process and Threat and Risk Assessments.	The CRA agrees with the recommendations. The CRA has a security evaluation process in place and continues to enhance this process based on evolving Treasury Board standards. The existing C&A processes will be enhanced to ensure security evaluations for all Agency applications as follows: • For future enterprise applications, the launch of a revised Security Assessment and Authorization (SAA) process which is consistent with the Treasury Board standard will ensure that newly developed applications will undergo complete C&A activities. It will be implemented by March 2014. • For existing enterprise applications, CRA conducts an Annual Status Update of all security evaluations that were completed since 2008. A review of all existing applications is underway and outstanding security evaluations are being prioritized and addressed. Timeframes to complete the outstanding security evaluations, for applications identified as high priority, will be in place by March 2014. • For local applications, a Local Application Repository (LAR) web application is in place to ensure that proper security evaluations are completed and tracked in accordance with the enhanced governance process described in our response to the recommendation at paragraph 55 (of the report).
The Canada Revenue Agency should: • Ensure that its policies, practices and procedures are followed to manage local applications and adequate safeguards are used to protect the taxpayer information they contain; • Ensure that its Local Application Repository is reviewed regularly for completeness, accuracy and currency; and • Follow up at each stage of the review and quality assurance processes and ensure that all local applications are approved by delegated officials before implementation.	The CRA agrees with the recommendations. A review of the existing procedures and safeguards coupled with a current state assessment of the Local Application Repository (LAR) is targeted for completion by the end of July 2013. There will be an action plan in place by the end of September 2013 to address any gaps. The governance process will be enhanced to include a mandatory review and approval process focusing on confirmation that privacy impact assessments and technical security reviews are completed prior to deployment in order to ensure completeness, accuracy, and currency. By the end of September 2013 all local application owners will be notified of the enhanced governance oversight.

Employee Access and Monitoring	
RECOMMENDATION	**AGENCY'S RESPONSE**
The Canada Revenue Agency should continue to enhance its Identity and Access Management System controls to ensure that employee access is limited to only that information required to carry out their job functions, based on the need-to-know principle.	The CRA agrees with the recommendation and will leverage the work that has been completed to date through the Identity and Access Management project, which includes the creation of the information resources completed March 2012, and the authoritative identity store implemented May 2013, and will: • continue to advance work already underway to review the roles and profiles used by managers to provision their employees which will be completed by October 2014; • implement an enhanced annual verification process which will be completed by December 2014; • continue implementing the remaining stages of the Identity and Access Management project and program. To date the CRA has invested approximately $10.5M and is planning a further significant investment to tackle this issue through both the Identity and Access Management as well as the Modernization of the National Audit Trail System projects.
The Canada Revenue Agency should review existing generic user IDs to determine whether they are required, authorized and controlled; and should delete all IDs that are not in use. The Canada Revenue Agency should also ensure that all generic user IDs are subject to established review and approval processes.	The CRA agrees with the recommendations and will: • strengthen the current process to introduce enhanced controls which will significantly reduce the number of generic accounts created which will be completed by December 2013; • leverage the authoritative identity store already implemented in May 2013 to conduct a full review of all existing generic accounts and take necessary action including the deletion of those not in use and the assigning of accountability for each account to named individuals which will be completed by March 2014; • enhance the security awareness and accountability surrounding generic accounts which will be completed by December 2014.

RECOMMENDATION	AGENCY'S RESPONSE
The Canada Revenue Agency should continue to strengthen its audit logging system and process and the Agency should incorporate risk assessment tools to flag potentially inappropriate employee activities on its systems.	The CRA agrees with the recommendation and will continue to strengthen its audit logging system and process capability by: • completing the implementation of the new Audit Trail Record Analysis Tool to assist management with the review of employee accesses which will be completed by December 2013; • furthering the ongoing work to enhance technological tools and associated business processes to proactively analyze user transactions, provide for early identification of issues, and detect certain patterns of behaviour. As noted in recommendation at paragraph 63 (of the report), to date the CRA has invested approximately $10.5M and is planning a further significant investment to tackle this issue through both: the Identity and Access Management as well as the Modernization of the National Audit Trail System projects.
The Canada Revenue Agency should ensure adequate measures are in place to mitigate the risks associated with developer access to taxpayer information in test environments. The Canada Revenue Agency should also rigorously control, track and monitor transfers of taxpayer information from operational to test environments.	The CRA agrees with the recommendations. The CRA will increase the control environment specifically around the use of taxpayer data in test environments by: • updating and communicating its policy suite concerning populating and accessing taxpayer data in test environments. This will be concluded by March, 2014; • developing an options analysis which will identify the most effective method to control, track and monitor transfers of taxpayer information from operational to test environments. This options analysis will be completed by March 2014, with implementation of the approved option immediately following.

Privacy Breaches	
RECOMMENDATION	**AGENCY'S RESPONSE**
Consistent with Treasury Board Guidelines for Privacy Breaches, the Canada Revenue Agency should ensure that the Access to Information and Privacy Directorate is notified of all breaches as they are discovered.	The CRA agrees with this recommendation and continues to enhance its established information-sharing protocol by: • immediately expanding the existing protocol to include the notification of all breaches in accordance with the Treasury Board Secretariat Guidelines on Privacy Breaches; • ensuring more timely breach notifications to the Access to Information and Privacy Directorate (ATIP).