Office of the
Privacy Commissioner
of Canada

PERSONAL INFORMATION DISPOSAL PRACTICES IN SELECTED FEDERAL INSTITUTIONS

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

Section 37 of the *Privacy Act*

FINAL REPORT

2010

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. IP54-34/2010
ISBN 978-1-100-52314-9

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

Table of Contents

Main Points

WHAT WE EXAMINED

The Government of Canada collects personal information in support of public policy and to deliver programs and services. When records with no archival or historical value reach the end of their established retention period and/or data resides on obsolete computers, the information is disposed of. Our audit examined how selected federal institutions manage the destruction of personal information.

Library and Archives Canada provides records storage and related services to over 90 federal institutions. The services may include the destruction of non-archival records that have reached the end of their retention period. Library and Archives Canada carries out the destruction service after obtaining concurrence from the client institution. We examined its off-site paper waste destruction program and the contractual arrangements with private shredding companies. We reviewed policies, procedures, threat and risk assessments, contracting files and associated records.

The audit also examined the disposal of surplus computers through donations to the Government of Canada's Computers for Schools program, as well as through public auction by Public Works and Government Services Canada – Crown Assets Distribution. We reviewed program records, observed processes and practices at Computers for Schools facilities, and tested surplus computers originating from federal institutions.

WHY THIS ISSUE IS IMPORTANT

The legislative mandates of federal departments and agencies allow for the collection of sensitive personal information. Whether applying for Canada Pension or Old Age Security benefits, completing census forms or filing personal income tax returns, individuals are not generally in a position to oppose the collection and use of their personal information by the federal government.

Implementing controls to ensure personal information is disposed of securely is a critical component in managing records. The unauthorized disclosure of personal information could have serious consequences for individuals, including financial loss resulting from identity theft or fraud, humiliation or damage to the individual's reputation, or risk to personal safety.

Federal departments and agencies have an obligation under the *Privacy Act* to protect information awaiting disposal with the same degree of care that is provided when the information is used for program and service delivery. This is essential for the government to maintain public trust in its ability to preserve the confidentiality of information that has been entrusted to it.

WHAT WE FOUND

We found that Library and Archives Canada has a comprehensive set of administrative policies and procedures for the disposal of federal government records. These are consistent with the requirements of the *Privacy Act*, the *Library and Archives of Canada Act* and Treasury Board policies, directives and standards.

Library and Archives Canada has implemented measures to ensure that personal information awaiting disposal is secure. The method of handling documents destined for off-site destruction sites is similar in the regions visited, resulting in a uniform process for the preparation and transportation of records.

However, we found that Library and Archives Canada is not systematically monitoring the destruction practices of off-site shredding companies. Documents revealed that two of the four shredding companies have violated their contractual obligations. Specifically, contract staff handling the destruction of records did not possess the requisite security clearance, the size of shredded material did not meet contract requirements, and documents were not disposed of within the prescribed timeframe.

Treasury Board policy requires federal departments and agencies to dispose of surplus assets in a manner that protects against the disclosure of sensitive information. Functional computer equipment that is deemed surplus within the federal government is either donated to the Computers for Schools program or sold through Public Works and Government Services Canada – Crown Assets Distribution.

The Computers for Schools program is operated by not-for-profit organizations under agreements with Industry Canada. The program collects and refurbishes donated surplus computers from various sources and distributes them to schools, libraries and not-for-profit learning organizations. Industry Canada is responsible for the management of federal equipment contributions to the program.

Under Treasury Board policy, departments and agencies are responsible for purging information on surplus computers prior to donating the equipment to the Computers for Schools program. In 1994-1995, the Privacy Commissioner reported that federal institutions were not complying with this policy requirement. The deficiencies noted 15 years ago persist today. We found multiple computers that contained personal information (including names, addresses, dates of birth and social insurance numbers), classified information and/or documents that were subject to solicitor-client privilege. The information residing on a number of hard drives was so sensitive that we took immediate steps to have them returned to the originating department.

Separate and related to this, while adequate Computers for Schools policies and procedures are in place, we found that Industry Canada has not established a protocol for analyzing and addressing security weaknesses that are reported to it by Computers for Schools workshops and warehouses in Annual Security Questionnaires.

Public Works and Government Services Canada – Crown Assets Distribution disposes of a small number of surplus federal computers, relative to the volume of computers that are donated to the Computers for Schools program. Many of the computers sold through Crown Assets Distribution do not contain hard drives, thereby mitigating any risk of a privacy breach. In addition, disposing institutions must certify in writing that all surplus assets have been cleansed of designated and classified information. Crown Assets Distribution will not dispose of an asset without this certification. When considered collectively, the above factors mitigate the risk of a data exposure resulting from the sale of a surplus computer.

Library and Archives Canada and Industry Canada have responded. Their responses follow the recommendations throughout this report.

Introduction

1. The disposal of records managed by federal government institutions occurs under the *Library and Archives of Canada Act*. The Act establishes the authority of the Librarian and Archivist of Canada to control the destruction of information and preserve government records with archival or historical value.

2. The Librarian and Archivist of Canada issues Records Disposition Authorities (RDA) to enable federal institutions to carry out their disposal plans. The RDA does not constitute a requirement to destroy records; it permits the destruction of documents that do not need to be preserved for future archival or historical use. The following principles guide the decision to destroy non-archival and non-historical records:

   - the information is no longer required for the purpose for which it was obtained or compiled; or
   - further retention of the information might unfairly prejudice the interests of the person to whom the information relates.

3. Federal institutions are accountable for ensuring that their records are disposed of in a secure manner. Library and Archives Canada (LAC) provides records storage and related services to approximately 90 federal entities. Once written consent to dispose of records has been received from the Librarian and Archivist of Canada, the decision on when and how to destroy records which do not have archival or historical value rests with the Deputy Head of a government institution. As part of the services offered by Regional Service Centres (RSCs), LAC will destroy records for clients. In some cases, these records have been stored in the RSCs and reached the end of their retention period; in others they are transferred to the RSCs from the creating institution for destruction only. When LAC accepts this role, it assumes responsibility for the secure disposal of the records. If LAC does not have written consent to proceed with the disposal action, the records are returned to the originating department or agency for disposal. At that point, the department or agency is accountable for implementing a secure disposal mechanism.

4. The federal government purchases large quantities of computers annually to replace obsolete equipment, which in turn generates a significant volume of surplus computers for disposal. Computers that have reuse potential are disposed of by way of donation to the Computers for Schools (CFS) program, which is operated by not-for-profit organizations under contribution and license agreements with Industry Canada. Industry Canada is responsible for developing and communicating national CFS program standards, including policies relating to security and computer cleansing processes. Surplus computers may also be transferred to Public

Works and Government Services Canada – Crown Assets Distribution for sale through public auction. Regardless of the disposal method used, the originating department or agency is responsible for purging (wiping) data stored in the memory of surplus computer equipment prior to its disposal.

5. Public Works and Government Services Canada (PWGSC) may also have a role in the disposal of paper records. The department provides support services to federal institutions, including contracting (procurement) arrangements with records destruction (shredding) companies. The Industrial Security Program within PWGSC was established to safeguard protected and classified government assets, including information. In terms of records disposal, the Program fulfills this role by ensuring records destruction companies have the necessary security clearances and they comply with security provisions established in contracts.

INADEQUATE DISPOSAL OF PERSONAL INFORMATION HAS BEEN AN ISSUE

6. The absence of controls surrounding the disposal process was the subject of one of the most serious violations of privacy investigated by the Office of the Privacy Commissioner (OPC). In July 1998, several tonnes of confidential and classified information about thousands of Canadians – which was collected by the federal government – were found in a company warehouse baled and ready for shipment abroad. The company had been hired to shred and recycle the records but was offering the material intact to the highest bidder because whole paper yielded a higher return than the sale of shredded paper on the recycling market.

7. This material included personal income tax records, immigration case files, parole records and employee pension files. Some of the documents were sent to the shredding company by National Archives Canada for disposal under a contract arranged by PWGSC.

8. There was clear evidence that National Archives of Canada and PWGSC were aware of the company's financial, security and technical problems before granting it a security clearance to transport and shred federal records. The OPC made a number of recommendations at that time, including that:

   - National Archives of Canada use off-site shredding services only if the companies could guarantee adequate security measures, and only if the shredding was under constant supervision; and
   - PWGSC examine its security clearance processes for contracts requiring the handling of personal information, and ensure that contracts include appropriate confidentiality provisions.

9. History also shows that federal departments and agencies have not consistently purged data from surplus computers. The Computers for Schools (CFS) program – founded in 1993 and managed by Industry Canada – collects, repairs and refurbishes donated surplus computers from government and private sector sources and distributes them to schools, public libraries and not-for-profit learning organizations throughout Canada. To date, CFS has refurbished and distributed over one million computers.

10. The Privacy Commissioner's 1994-1995 Annual Report noted that approximately 95 percent of all computers donated by federal institutions to the CFS program had data and programs residing on them, despite Treasury Board policy requiring that computers be cleansed prior to donation. While the following year showed progress (35-45 percent of computers were wiped), the Commissioner observed that there was still room for improvement.

FOCUS OF THE AUDIT

11. The objective of the audit was to assess whether LAC, Industry Canada – Computers for Schools program, and PWGSC have implemented adequate policies, procedures, processes and controls to ensure that personal information is disposed of in a secure manner. A secure disposal method provides assurance that the information cannot be retrieved or reconstructed.

12. These entities have a role in the disposal of information or surplus assets on behalf of other federal departments and agencies. The audit focused on their respective roles in this regard.

13. The audit did not include an examination of the personal information disposal practices of the federal departments and agencies that rely on the three audited entities for the disposal of information or surplus assets. Further, while the examination included visits to private sector shredding companies and Computers for Schools facilities, the audit was not designed to examine their business operations in significant detail. Information on the scope, criteria and approach of the audit can be found in the **About the Audit** section of this report.

Observations and Recommendations

OFF-SITE DISPOSAL OF RECORDS ON BEHALF OF LIBRARY AND ARCHIVES CANADA

14. Section 6(3) of the *Privacy Act* requires government institutions to dispose of personal information in accordance with the Regulations and with any directives or guidelines issued by the Treasury Board. Maintaining the security of personal information is a key component in meeting protection requirements established under the Act. Appropriate measures and controls must be present to ensure personal information is not compromised during its life cycle – from the time of collection until it is destroyed by an approved method.

15. The Policy on Government Security and its related standards establish baseline (minimum) safeguards to protect and preserve the confidentiality and integrity of government assets, including personal information. Federal institutions are required to conduct their own assessments to determine whether measures above baseline levels are warranted.

Management of security aspects surrounding off-site shredding contracts generally comply with Treasury Board policy

16. Treasury Board policy requires that a contractor be security cleared at the appropriate level prior to commencing work. The Security and Contracting Management Standard allows for one exception to this general rule: where supported by a threat and risk assessment, the step of ensuring that a contractor meets the security requirements before the contractor is granted access to designated information may be replaced by a clause in the contract. The delay clause should stipulate that all security requirements must be met within six months after the contract is awarded.

17. We examined the contracting files of the four private sector entities that provide off-site document destruction services to Library and Archives Canada (LAC). We expected to find that their facilities and personnel had been granted the required security clearances prior to commencing any contract work. We also expected to find key security screening documents on file.

18. Companies under contract with the government must sign a Security Agreement with Public Works and Government Services Canada (PWGSC). The Agreement places the responsibility for safeguarding government information on the company's chief security officer (CSO). The CSO is also required to sign a Security Screening Certificate and Briefing Form, acknowledging and agreeing to comply with all requirements associated with the security clearance. A Security Requirements Checklist is mandatory for all contracts for which PWGSC is the contracting authority. This Checklist defines the terms and conditions to be included in the contract to ensure sufficient and appropriate controls are in place to protect government assets.

19. All of the contract files we examined contained a signed Security Screening Certificate and Briefing Form, as well as a Security Requirements Checklist. A Security Agreement was retained on three of the four files.

20. We found one off-site shredding contract that was awarded approximately six months before the contractor was cleared to the required security level. The agreement, signed by PWGSC and the shredding company in 2001, established an off-site records destruction program for a number of federal departments and agencies, including LAC. The agreement did not include a delay clause as required under Treasury Board's Security and Contracting Management Standard, nor was the delay supported by a threat and risk assessment. As the contracting officer was no longer employed by PWGSC at the time of the audit, we were unable to verify the circumstances surrounding the decision to allow the shredding company to commence work before the security clearance was granted. The contract was extended in 2007 and again in 2009. The required site and personnel clearances were in place on both occasions.

Adequate controls are in place to protect personal information awaiting disposal

21. Treasury Board's Operational Security Standard on Physical Security establishes processes and controls to manage protected and classified assets awaiting destruction. They include appropriate storage facilities to prevent unauthorized access, theft or loss, and measures to protect records from the time they leave the organization until their destruction. We expected LAC to have protocols in place to meet all requirements established under the Standard.

22. We examined relevant policies and procedures and interviewed LAC employees at five Regional Service Centres. We conducted site visits in two regions in order to observe the preparation and transportation of records from LAC to off-site shredding companies. We visited these companies and received briefings on their disposal processes and the measures used to protect records awaiting destruction.

23. We found that LAC has a comprehensive set of administrative policies and procedures for the disposal of records. The method of handling documents destined for off-site destruction is similar in the regions visited, resulting in a consistent process for safeguarding records in transit.

24. Documents are placed in boxes, segregated and stored in a secure area with restricted access. Once a sufficient number of records are assembled, arrangements are made with the shredding company for their removal. Designated LAC employees monitor the entire removal process and verify that the vehicle door is padlocked and security sealed once the loading process is complete. A way bill is prepared, with the seal number recorded on it. All contracts stipulate that records are to be transported to the contractor's facility without delay.

25. Upon arrival at the shredding facility the waybill is stamped and a copy, with the security seal attached, is returned to LAC confirming receipt of the documents. The records are then moved to a designated area for processing. All of the shredding companies we visited had a secure room for storing and shredding LAC records.

26. On the basis of our review of off-site shredding contracts and established policies and procedures, we conclude that adequate controls exist to protect personal information destined for destruction.

Uniform shredding specifications for protected information are not in place

27. Treasury Board's Operational Security Standard on Physical Security provides baseline (minimum) physical security requirements to ensure protected and classified records are destroyed in a secure manner. These requirements are intended to make the reconstruction of information on shredded paper impracticable.

28. For the purposes of this audit, our inquiries focused on the off-site destruction of Protected A and Protected B information. Protected B records are particularly sensitive, the unauthorized disclosure of which could reasonably be expected to cause serious injury to an individual, organization or government.

29. LAC also manages the disposal of classified information, the unauthorized disclosure of which could cause injury to the national interest. However, these records are destroyed on-site within a very controlled environment.

30. Treasury Board policy establishes a strip-cut to a maximum width of 3/8 of an inch (10mm) as the minimum shredding standard for information designated as Protected A and Protected B. We expected to find that all contracts would have uniform specifications to meet or exceed the minimum standard.

31. We found that contract requirements varied. Two of the contracts required protected material to be shredded to a maximum width of 6.36 mm (¼ inch) strips or less. This is consistent with LAC's own Security Standard, which states:

> Paper records are to be destroyed in a secure environment and in a timely manner by pulping, or by shredding into ¼ inch strips maximum.

32. One of the two remaining contracts had a shredding requirement of 3/8 inch strips or less, the minimum under Treasury Board policy. The other required material to be "cross cut": shredded at a 3/8 inch at any length and then shredded a second time using a 5/8 inch shred width. One company provides records destruction services to LAC in two regions. The contracts have different shredding specifications.

33. Although Treasury Board policy establishes baseline (minimum) shredding specifications, federal departments and agencies may implement safeguards above the baseline standards. LAC has concluded that a shredding specification above the minimum standard is required to ensure that sensitive documents cannot be reconstructed. Consequently, it has embedded a more stringent requirement – ¼ inch strip shredding – into its Security Standard. This requirement is not consistently applied.

34. RECOMMENDATION

> Library and Archives Canada should ensure that the terms and conditions in off-site destruction contracts are consistent with its own Security Standard.

Library and Archives Canada response: In consultation with Public Works and Government Services Canada and LAC Corporate Security Services, LAC's contracting officers will ensure that all contracts issued for off-site shredding services will include uniform shredding specifications that meet or exceed LAC's minimum security standards.

The destruction of records is not systematically monitored

35. Treasury Board's Security and Contracting Management Standard states that departmental policies and procedures should provide for scheduled and unscheduled inspections of contractor work sites, and for the safeguarding of sensitive waste until it is destroyed by an approved method. To satisfy Treasury Board policy requirements and to mitigate the risk of another data breach (paragraphs 6 and 7 of this report refer), the National Archivist, in a letter addressed to the Privacy Commissioner in 2002, provided assurance that LAC would implement a rigorous and detailed audit protocol for off-site records destruction contracts.

36. We expected to find an effective monitoring regime in place, with supporting records to demonstrate that LAC is systematically monitoring off-site shredding companies through periodic inspections and annual audits. While we were told that inspections are generally performed annually, LAC was unable to produce evidence to support this assertion. The records that LAC did provide, as well as our review of inspection reports prepared by PWGSC, underscore the importance of systematic compliance monitoring.

Shredding company suspended from the Industrial Security Program

The Industrial Security Program of PWGSC issues site and personnel security clearances to contractors requiring access to protected information, assets or restricted work sites and/or document safeguarding capability for protected material. A contractor must satisfy prescribed security criteria before the clearance is granted.

PWGSC conducts follow-up (renewal) inspections every two years to ensure that contractors continue to meet all security requirements. A site clearance – and the ability to handle protected information – may be suspended if a contractor fails to address deficiencies noted during the inspection.

A PWGSC industrial security officer conducted a renewal inspection of a shredding company in September 2009. The inspector identified a number of deficiencies that placed the company in non-compliance with its contractual obligations. Specifically, employees were not appropriately security screened and the average width of shredded material exceeded contract specifications by 50 percent. Records on file suggest that the company was in non-compliance for a number of years.

The entity was provided 90 days to address the deficiencies. When the company did not respond, it was suspended from the Industrial Security Program. The suspension was lifted once PWGSC verified that corrective measures were implemented to satisfy all security requirements.

Company violates key contract requirements

An unannounced inspection of a shredding company was carried out by LAC in 2002, with a follow-up two years later. LAC officials were initially denied access to the facility, contrary to contract requirements. When access was provided, the inspectors located full pallets of material that were transported for destruction 12 days earlier. These records should have been destroyed within 72 hours of receipt, as prescribed under the contract.

37. In summary, two of the four companies providing off-site destruction services to LAC have violated their contractual obligations. This is significant given that the areas of non-compliance related to key components of a secure off-site disposal process, specifically:

    - individuals who have access to sensitive information are screened to the appropriate level;
    - information is destroyed in a manner that it cannot be reconstructed; and
    - records are disposed of in a timely basis to mitigate the risk of unauthorized access.

38. In the absence of evidence to the contrary, it would appear that accountability for meeting the National Archivist's 2002 commitment, insofar as monitoring off-site records destruction contracts, has not been clearly established within LAC and communicated to the appropriate staff.

39. The responsibility for ensuring that unannounced inspections and audits are carried out and recorded must be well understood. Without clear accountability and enforcement, shredding companies may circumvent contract requirements.

40. Furthermore, measuring compliance with contract requirements presupposes an administrative infrastructure that tracks the entire destruction process. With one exception, shredding companies are not required to submit a signed declaration to LAC, recording the date upon which records are destroyed. This declaration is commonly referred to as a certificate of destruction. Requesting this certificate, along with systematic monitoring activities, would demonstrate that LAC is exercising due diligence by ensuring shredding companies comply with their contractual obligations.

41. RECOMMENDATION

Library and Archives Canada should: implement a protocol for monitoring off-site records destruction companies to provide assurance that privacy and security requirements are being met in a consistent manner; and ensure that off-site destruction contracts include a requirement that the service provider issue a certificate of destruction, recording the date records are destroyed and the name of the authorized contractor personnel who conducted/witnessed the destruction.

Library and Archives Canada response:
Standard clauses will be included in off-site shredding contracts to ensure an adequate level of periodic monitoring activities. This will include a standard clause requiring that service providers issue certificates of destruction, recording the date records are destroyed and the name of the authorized contractor personnel who conducted/witnessed the destruction.

LAC contracting officers will work diligently with LAC's Corporate Security Services and Public Works and Government Services Canada to develop effective and efficient monitoring mechanisms to ensure consistency with privacy and security requirements set out in contracts.

LAC Corporate Security Services will manage periodic inspections of off-site shredding companies within the National Capital Region (NCR) in collaboration with Material Management and Regional Service Centres (RSCs) located in the NCR. Corporate Security Services will develop a verification tool and work in collaboration with LAC RSCs to perform inspections in other locations in Canada.

Contract files will be properly documented to demonstrate compliance with contract terms and conditions.

INDUSTRY CANADA – COMPUTERS FOR SCHOOLS

42. The Computers for Schools (CFS) program was created in 1993. It is operated by not-for-profit organizations under contribution and license agreements with Industry Canada. The program collects and refurbishes donated surplus computers from federal, provincial and municipal governments, private sector companies and individuals. The refurbished equipment is distributed to schools, libraries, not-for-profit learning organizations, as well as Aboriginal communities. There are over 40 CFS workshops and warehouses across Canada.

43. Industry Canada is responsible for developing and communicating national CFS program standards, including policies relating to security and computer cleansing processes. CFS licensees must ensure that such policies are implemented and national standards are followed.

44. Treasury Board's Directive on the Disposal of Surplus Material requires federal departments and agencies to offer the CFS program right of first refusal of all surplus IT equipment. This includes computers, laptops, servers, printers, modems, hard drives and network cards.

Policy and procedural controls are in place

45. There is always a risk that surplus computer equipment may contain protected or classified information if it is not cleansed. While data security is the responsibility of the donating institution, any inadvertent exposure of information could compromise security, privacy and undermine the integrity of the CFS program. Therefore, we expected to find policies, procedures and controls to mitigate this risk.

46. We examined CFS security policies and procedures, as well as agreements between Industry Canada and CFS licensees. These documents address roles, responsibilities and reporting requirements in significant detail, and prescribe baseline measures to ensure that physical, personnel and information technology security requirements of the program are met.

47. While sound policies and procedures are in place, Industry Canada does not reconcile the number of computers that are donated by federal institutions under the CFS program with the number that are cleansed through the CFS refurbishment process. Statistical reports are designed to measure production (computers shipped to CFS clients), not where computers originated. In the absence of a reporting mechanism, computers may be lost or stolen with no means of detection. This is noteworthy given that surplus computers are not consistently cleansed prior to being sent to CFS facilities – paragraph 54 of this report refers.

Deficiencies highlighted in security questionnaires are not consistently addressed

48. CFS contribution agreements and security policy require workshops and storage areas to have appropriate safeguards to prevent unauthorized access to surplus equipment. CFS workshops may have unique protection requirements due to their physical location, line of business and asset inventory. As security needs may vary, all CFS licensees must complete an annual security self-assessment. The results are recorded on a CFS Workshop Security Questionnaire and submitted to Industry Canada.

49. The questionnaires are used to develop CFS facility security profiles, assess compliance with CFS security policy, and recommend corrective measures as required. Industry Canada may also use the information for site inspection purposes. We examined security questionnaires submitted during 2008-2009 and 2009-2010. A significant number of questionnaires included responses indicating non-compliance with CFS policy. The deficiencies generally related to the storage and tracking of hard drives, and employee security screening.

50. As the questionnaires highlight potential security vulnerabilities, we examined whether they are subject to systematic analysis and follow-up with CFS licensees. Our examination of files and discussions with Industry Canada staff confirmed that they are not. The questionnaires provide key indicators of non-compliance with program security requirements. Deficiencies that are not addressed could place program assets, including personal information, at risk.

51. RECOMMENDATION

Industry Canada should establish a mechanism to ensure that all reported security weaknesses at Computers for Schools workshops are analyzed and addressed in a timely manner.

Industry Canada response: While mechanisms are already in place (i.e. in-person site visits), the Computers for Schools Program agrees with the report's findings and recommendations that improvements could be made. The Program will be developing a plan by the end of the third quarter of the 2010/2011 fiscal year to address this problem.

Sensitive data found on computers donated by federal institutions

52. Treasury Board policy requires departments and agencies to purge all computers of classified and protected information prior to disposal. While the CFS program is the recipient of donated surplus equipment, it is not part of its mandate or role to enforce this Treasury Board policy requirement.

53. Within the CFS context, surplus computers are considered disposed of at the time departments and agencies surrender ownership of the equipment to the CFS program. We examined whether computers were cleansed of data prior to being transported to CFS facilities.

54. We carried out audit testing at CFS workshops in Halifax, Truro, Gatineau, Toronto, Winnipeg and Vancouver. A sample of 1,093 computers was selected for this purpose. The sample included computers originating from 31 federal institutions. Of the 1,093 computers tested, 458 (approximately 42 percent) contained hard drives that were not completely erased by the department or agency prior to being donated to the CFS program, thereby contravening Treasury Board policy. Of these, 123 drives were taken into evidence for analysis. Detailed forensic analysis was performed on a selection of the drives. The information residing on a number of them was so sensitive that we took immediate steps to have the hard drives returned to the originating department.

Information found on computer hard drives included:

- Names, addresses, dates of birth, and social insurance numbers of individuals seeking access to various government programs and services;
- Records subject to solicitor-client privilege;
- Classified information; and
- Personal files of federal public servants.

55. The CFS program was not designed or intended to be a computer hard drive cleansing service for federal institutions. If such a mandate had been envisioned, CFS facilities and personnel would be subject to the same security screening processes that contractors must undergo prior to being granted access to protected and classified government information.

56. The audit shows that federal departments and agencies are not exercising due diligence in ensuring computers are cleansed prior to donating them to the CFS program, despite Treasury Board policy requiring that this be done. It also demonstrates that the deficiencies highlighted by the Privacy Commissioner fifteen years ago persist today. Until this is addressed, Canadians' privacy will remain at risk.

57. RECOMMENDATION

Industry Canada should work with the Treasury Board Secretariat to request that federal departments and agencies provide a signed declaration to the Computers for Schools program certifying that all donated surplus computers and related assets have been cleansed of protected and classified information.

Industry Canada response: While it is not the Program's mandate/responsibility to ensure that surplus computers have been cleansed of protected and classified information, the CFS Program is well positioned to play a role in supporting the Treasury Board Policy and encouraging federal departments and agencies to exercise due diligence in ensuring that computers are cleansed prior to donating them to the Program.

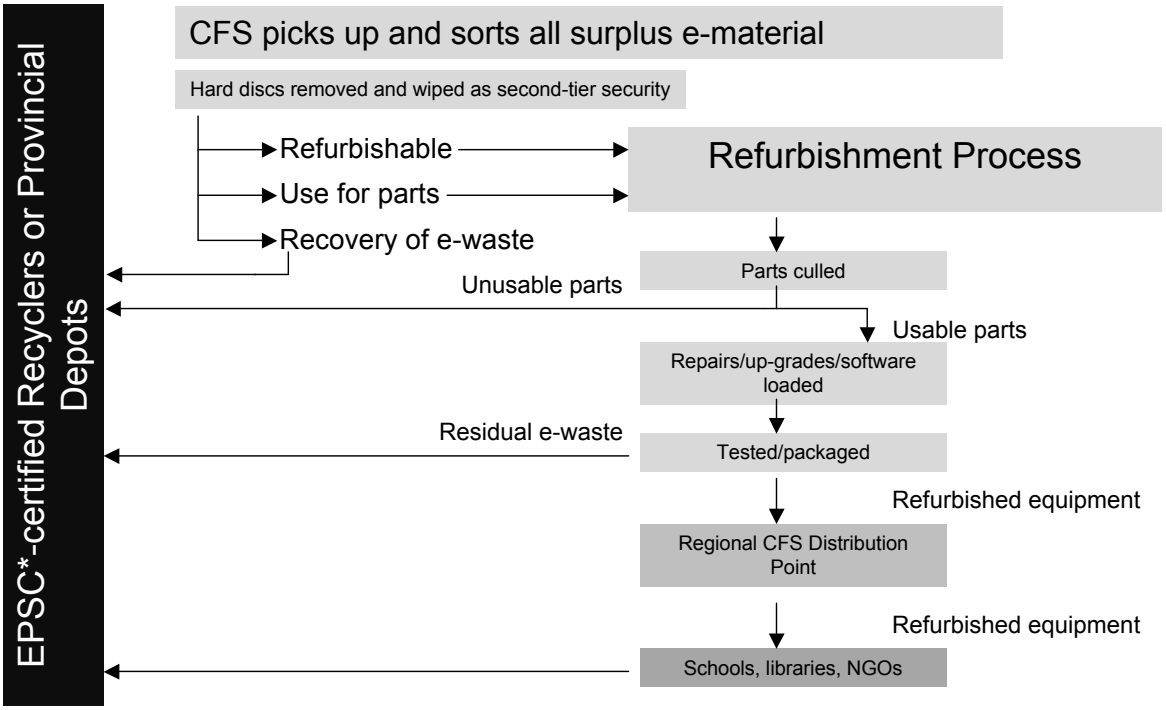
The Computers for Schools Program will work collaboratively with Treasury Board, as well as with all other federal departments and agencies, on the development and implementation of a new surplus certification report.

The CFS will conduct consultation sessions with parties involved in the fall 2010 and aim to have the new certification report implemented by April 2011.

Program provides level of assurance that data is erased on surplus computers

58. It was not within the audit scope to examine the operations of CFS workshops in significant detail. However, upon establishing that many computers donated by federal institutions contained sensitive data, we looked at the refurbishment processes at six CFS workshops in five regions. We examined whether controls exist to mitigate the risk of a data breach. We received briefings from workshop employees and observed the procedures used to process donated computers. We also tested a sample of refurbished units that were cleared for distribution to CFS clients.

59. Although the operating procedures for managing computer hard drives varied slightly among the workshops, we found that a standard refurbishment process is followed; this is described below.



Source: Industry Canada – Computers for Schools

60. While the onus is on the donor to ensure that all computer hard drives have been cleansed (wiped), CFS policy requires – as an additional precautionary measure – that all computers be cleansed prior to distribution. Hard drives are generally tagged upon receipt and sent to a wiping station to be overwritten (erased). Once a computer has been refurbished with a drive reinstalled, a second test is performed to verify that the hard drive has been cleansed. Software is then loaded, final performance tests are conducted and the unit is cleared for distribution. We randomly selected 414 hard drives for testing purposes and found that they were wiped.

61. Based on the audit work performed, we conclude that CFS operational procedures include sound controls to mitigate the risk of computers being distributed to clients with personal information residing on the hard drives.

PUBLIC WORKS AND GOVERNMENT SERVICES CANADA – CROWN ASSETS DISTRIBUTION

Compensating factors mitigate the risk of a data breach

62. As previously mentioned, federal departments and agencies must offer the CFS program right of first refusal of all surplus computers. If the equipment cannot be used by the program, it is transferred to Crown Assets Distribution (CAD), a Directorate within Public Works and Government Services Canada. CAD sells, distributes and disposes of surplus federal goods. Surplus assets may be sold on-site where they were declared surplus or at a CAD regional service centre. Sales are generally conducted through CAD's on-line auction web site.

63. Departments and agencies have sole responsibility for preventing the unauthorized release of information contained in surplus assets, regardless of the disposal mechanism used. Whether a surplus computer is donated to the CFS program or it is transferred to CAD for sale through public auction, accountability for ensuring the computer is cleansed of all classified and protected information rests with the originating (disposing) federal institution. CAD is not responsible for ensuring that institutions satisfy this obligation, nor is it funded to provide a computer hard drive sanitization (wiping) service to federal institutions. Furthermore, in many instances CAD does not take physical possession of the surplus equipment; it remains at the disposing institution until it is sold. We examined CAD's procedures and processes and tested surplus computers at one CAD warehouse; the other warehouses did not have computers in their inventory at the time of our site visits.

64. We found that a number of factors mitigate the risk of surplus computers being sold with data residing on them. One such factor is a requirement for disposing institutions to submit a Report of Surplus (ROS). The ROS lists the surplus equipment and departmental material managers must confirm that all security requirements have been addressed. By signing the ROS, the manager certifies that the surplus equipment is clear of all forms of classified and designated (protected) information. CAD will not dispose of any material without a signed ROS.

65. A small number of computers are disposed of through CAD, relative to the volume of computers that are disposed of by federal institutions under the CFS program. In 2009, federal donations to the CFS program exceeded 60,000 computers. By comparison, 1440 computers were sold through CAD. Moreover, the overwhelming majority of these computers, including those that we tested, were sold without hard drives.

66. While no system is infallible, the above compensating factors, when considered in concert, suggest that the disposal of computers through Public Works Government Services Canada – Crown Assets Distribution poses a minimal risk to privacy.

Conclusion

67. Section 6(3) of the *Privacy Act* requires government institutions to dispose of personal information in accordance with the Regulations and with any directives or guidelines issued by the Treasury Board. Maintaining the security of personal information until it is disposed of by an approved method is a key component in meeting protection requirements established under the *Act*.

68. Library and Archives Canada has a comprehensive set of administrative policies, procedures and practices for managing the disposal of federal government records. Security requirements embedded in off-site destruction contracts comply with Government policy, and they provide adequate controls to ensure records are transported, stored and disposed of in a secure manner.

69. While the establishment of sound policies, procedures and controls is critical, there must be ongoing assurance that they are being followed. Library and Archives Canada has been guided by the assumption that off-site shredding companies are complying with contract security requirements; however, there is no mechanism to provide assurance that this is so. In the absence of an effective monitoring regime, shredding companies may circumvent contract requirements designed to protect privacy, deliberately or otherwise, without consequence.

70. Federal departments and agencies have sole responsibility for preventing the unauthorized release of information contained in their surplus assets, regardless of the disposal mechanism used. The overwhelming majority of surplus computers are donated to the Computers for Schools program. Treasury Board policy requires that these computers be cleansed of all classified and protected information prior to donation. Of the computers we tested from 31 federal institutions, we found that 28 institutions (approximately 90 percent) had not fulfilled this obligation. A concerted effort is needed to strengthen accountability for compliance with this policy requirement. Until this is done, the privacy of Canadians will remain at risk.

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 determine whether selected government institutions have developed and implemented adequate controls – including policies and procedures – to ensure personal information is disposed of in a secure manner.

CRITERIA

Audit criteria are derived from the *Privacy Act*, *Library and Archives of Canada Act*, the Policy on Government Security and related standards.

We expected to find that:

- adequate policies and procedures are in place to safeguard personal information destined for disposal;
- disposal practices comply with requirements prescribed under the Policy on Government Security and Operational Security Standard on Physical Security;
- off-site destruction of records satisfy contract security requirements, and private sector entities performing such services are subject to ongoing monitoring and audit; and
- surplus computers are cleansed of all data prior to being donated to the Computers for Schools program or sold through Public Works and Government Services Canada – Crown Assets Distribution.

SCOPE AND APPROACH

Library and Archives Canada, Public Works and Government Services Canada and Industry Canada – The Computers for Schools program have a role in respect of the disposition of records or surplus assets on behalf of other federal institutions. The examination was tailored to their respective roles in this regard, with a focus on the measures – policies, procedures, processes and controls – in place to ensure personal information is disposed of in a secure manner.

Audit evidence was obtained through various means, generally involving on-site examinations, interviews and information obtained through correspondence. We also reviewed policies, procedures, supporting systems and files. Finally, we tested surplus computers donated by federal institutions under the Computers for Schools program.

Audit activities were carried out at Library and Archives Canada and Public Works and Government Services Canada within the National Capital Region and in Halifax, Dartmouth, Toronto, Winnipeg and Vancouver. We also visited six Computers for Schools workshops and three private sector companies that provide off-site records destruction services to Library and Archives Canada. The selection of specific sites was be made following consultation with departmental officials.

The audit work was substantially completed on March 31, 2010.

STANDARDS

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

AUDIT TEAM

Director General: Steven Morgan

Michael Fagan
Bill Wilson

Subhas Roy (Consultant)
Matthew Williams (Consultant)

Appendix – List of recommendations

RECOMMENDATION

Library and Archives Canada should ensure that the terms and conditions in off-site destruction contracts are consistent with its own Security Standard.

RESPONSE

In consultation with Public Works and Government Services Canada and LAC Corporate Security Services, LAC's contracting officers will ensure that all contracts issued for off-site shredding services will include uniform shredding specifications that meet or exceed LAC's minimum security standards.

RECOMMENDATION

Library and Archives Canada should: implement a protocol for monitoring off-site records destruction companies to provide assurance that privacy and security requirements are being met in a consistent manner; and ensure that off-site destruction contracts include a requirement that the service provider issue a certificate of destruction, recording the date records are destroyed and the name of the authorized contractor personnel who conducted/witnessed the destruction.

RESPONSE

Standard clauses will be included in off-site shredding contracts to ensure an adequate level of periodic monitoring activities. This will include a standard clause requiring that service providers issue certificates of destruction, recording the date records are destroyed and the name of the authorized contractor personnel who conducted/witnessed the destruction.

LAC contracting officers will work diligently with LAC's Corporate Security Services and Public Works and Government Services Canada to develop effective and efficient monitoring mechanisms to ensure consistency with privacy and security requirements set out in contracts.

LAC Corporate Security Services will manage periodic inspections of off-site shredding companies within the National Capital Region (NCR) in collaboration with Material Management and Regional Service Centres (RSCs) located in the NCR. Corporate Security Services will develop a verification tool and work in collaboration with LAC RSCs to perform inspections in other locations in Canada.

Contract files will be properly documented to demonstrate compliance with contract terms and conditions.

RECOMMENDATION

Industry Canada should establish a mechanism to ensure that all reported security weaknesses at Computers for Schools workshops are analyzed and addressed in a timely manner.

RESPONSE

While mechanisms are already in place (i.e. in-person site visits), the Computers for Schools Program agrees with the report's findings and recommendations that improvements could be made. The Program will be developing a plan by the end of the third quarter of the 2010/2011 fiscal year to address this problem.

RECOMMENDATION

Industry Canada should work with the Treasury Board Secretariat to request that federal departments and agencies provide a signed declaration to the Computers for Schools program certifying that all donated surplus computers and related assets have been cleansed of protected and classified information.

RESPONSE

While it is not the Program's mandate/responsibility to ensure that surplus computers have been cleansed of protected and classified information, the CFS Program is well positioned to play a role in supporting the Treasury Board Policy and encouraging federal departments and agencies to exercise due diligence in ensuring that computers are cleansed prior to donating them to the Program.

The Computers for Schools Program will work collaboratively with Treasury Board, as well as with all other federal departments and agencies, on the development and implementation of a new surplus certification report.

The CFS will conduct consultation sessions with parties involved in the fall 2010 and aim to have the new certification report implemented by April 2011.