




Office of the
Privacy Commissioner
of Canada

Special Report to Parliament

Findings under the *Privacy Act*

Investigation into the loss of a hard drive at Employment and Social Development Canada

March 25, 2014



Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

© Minister of Public Works and Government Services Canada 2014

IP54-56/2014E-PDF
978-1-100-23322-2

Follow us on Twitter: [@PrivacyPrivee](https://twitter.com/PrivacyPrivee)



Contents

Investigation into the loss of a hard drive at Employment and Social Development Canada	1
Complaint Under the <i>Privacy Act</i>.....	1
Introduction	1
Background	1
Methodology.....	2
Summary of Facts.....	2
ESDC’s Actions Following the Incident.....	4
Application	9
Analysis.....	9
I. Physical Controls.....	10
II. Technical Controls.....	11
III. Administrative Controls	12
IV. Personnel Security Controls.....	13
Findings.....	14
Recommendations.....	15
Other Observations	21
Conclusion	22
Additional Information.....	23

Investigation into the loss of a hard drive at Employment and Social Development Canada

Complaint Under the *Privacy Act*

Introduction

1. This Report of Findings relates to a Commissioner-initiated complaint against Employment and Social Development Canada (ESDC), formerly Human Resources and Skills Development Canada (HRSDC), in relation to the loss of an external hard drive (the “incident”) containing the personal information of 583,000 Canada student loan borrowers, and 250 ESDC employees.

Background

2. On December 17, 2012, ESDC verbally notified our Office of the incident. Formal written notification was subsequently received from ESDC on January 7, 2013.
3. ESDC’s written notification advised that the external hard drive contained personal information dated from 2000-2006 for Canada Student Loan borrowers, including: Social Insurance Number (SIN), first name, last name, date of birth, home address, and telephone number. ESDC subsequently informed our Office that the external hard drive also included student loan balance information. In addition, the external hard drive contained employee information from a Business Continuity Plan fan out list. This information included first name, last name, home address and home phone number and/or cell phone number.
4. Upon receipt of the notification from ESDC, we determined that there were reasonable grounds for a Commissioner-initiated complaint against the Department to ascertain whether there has been a contravention of the *Privacy Act*.
5. Accordingly, the Office of the Privacy Commissioner of Canada (the “OPC”) initiated a complaint against ESDC on January 11, 2013, pursuant to subsection 29(3) of the *Privacy Act* (the *Act*).
6. The OPC’s investigation focused on the incident in relation to the disposal, use and disclosure provisions of the *Act*.

Methodology

7. Our investigation examined the circumstances surrounding the incident, as well as ESDC's policy framework in order to identify the degree of conformity with the applicable Government of Canada privacy-related policies, and whether the Departmental policies and procedures that were in place at the time of the incident were sufficient and effectively implemented.
8. To this end, we reviewed the representations received from ESDC in relation to the incident, and our investigation entailed interviews with key employees identified as having access to the missing external hard drive, as well as a site visit to ESDC's Canada Student Loans Program (CSLP) Unit, and meetings with Departmental officials.

Summary of Facts

9. The CSLP promotes accessibility to post-secondary education for students with a demonstrated financial need by lowering financial barriers and ensuring Canadians have an opportunity to develop the knowledge and skills to participate in the economy and society. With these objectives in mind, the CSLP offers a suite of student financial assistance programs and services, including student loans for full-time and part-time students, non-repayable grants, and repayment assistance measures for borrowers who experience difficulty repaying their loans.
10. The investigation confirmed that, on November 5, 2012, an employee of the CSLP Unit went to retrieve an external hard drive from a filing cabinet and noticed that it was missing.
11. According to ESDC's representations, the hard drive was stored in a lockable filing cabinet located in that employee's cubicle, in an envelope, hidden under suspended files.
12. ESDC reported that the external hard drive was a 1 terabyte (TB) Seagate GoFlex. It was not password protected, nor was the information contained on it encrypted. The serial number of the hard drive remains unknown.
13. According to ESDC, the external hard drive was used to backup information in preparation for the migration of information from the T drive to the U drive on the Department's network. The migration of information was performed by the Innovation, Information and Technology Branch (IITB) on October 12, 2012.
14. ESDC confirmed that the IITB was not involved in the backup of information on the hard drive, as the hard drive was not technically necessary for the data migration. The hard drive was only used as a risk mitigation measure by the CSLP to protect against inadvertent loss or deletion of the files during the migration.
15. By way of background, ESDC confirmed that the data migration project started in 2011 by the Operational Program Support Division (OPSD). The OPSD became the Program Integrity and Accountability (PIA) Division in the fall of 2011. The PIA Division provides stewardship to the CSLP through leadership in planning, reporting, portfolio management, accountability, program integrity and compliance, as well as administrative services for the CSLP, including finance, human resources, financial and information management, security and accommodations.

16. Following a comprehensive review of the files and folders on the Department's network that were identified for the migration project, ESDC informed our Office that the following data files were compromised by the loss of the external hard drive, each of which is described in more detail below:

- Files pertaining to client satisfaction surveys;
- Files containing investigation reports;
- Files containing CSLP financial, business plan and Human Resources information;
- Files containing Business Continuity Planning information.

17. Notwithstanding the above, as the hard drive is missing, ESDC submits that there is no way to conclusively identify what information was in fact backed up to the hard drive.

Client Satisfaction Surveys

18. The CSLP conducts an annual survey to track experience and satisfaction with CSLP service delivery for in-study borrowers and those borrowers in repayment. The survey is also used to measure satisfaction with service delivery by the National Student Loans Service Centre (NSLSC), and helps the CSLP better understand the client population. The PIA Division is responsible for the client satisfaction survey on behalf of the CSLP.

19. ESDC reported that some of the information contained on the hard drive stems from files associated with the CSLP's client satisfaction surveys that were conducted in 2004-2005, 2005-2006, and 2006-2007. ESDC subsequently confirmed that some of the affected borrowers fall beyond the survey years initially reported, up to and including the disbursement year 2012.

20. In addition to the seven pieces of personal information described by ESDC in its notification to our Office, the files relating to client satisfaction surveys may have also included the following fields of information in relation to borrowers:

Loan certificate number, loan ID number, loan class (whether the borrower is in study, or in repayment), whether the borrower had direct contact with the Service Provider, the name of the education institution that the borrower attended, the borrower's gender, language, marital status, the province that issued the loan, the type of loan (e.g. part time loan), years of study, end of study date, loan interest rate, loan interest type, the date the loan was issued, the disbursement date, the federal loan disbursement amount, the student loan consolidation date, whether the borrower is active (borrower sent in consolidation agreement), or passive (borrower did not submit consolidation agreement), the type of loan (eg. full-time direct, part-time direct, integrated), delinquency flag (identifies whether the borrower is in delinquency), the delinquency date, a 'paid in full' indicator, the outstanding balance on the loan, fax number.

21. ESDC submits that not all information fields were populated for each borrower. The personal information of the affected individuals on the external hard drive was contained within different data files and, as such, the number of information fields found within these files varied.

Investigation Reports

22. We confirmed that the "investigation reports", described by ESDC as part of the information content on the hard drive refer to the administrative investigations that were undertaken to confirm the eligibility of a number of students for the CSLP, including loans, grants, and repayment assistance.

23. ESDC submits that the following data elements were included in a series of working documents that itemized the individuals being reviewed for eligibility: client's name, address, SIN, date of birth and loan amount.
24. Our review confirmed that the hard drive may have also included the following fields of information in the investigation reports:
- Canada student loan number, amount paid (including interest), amount paid to principal only, and status (this indicates whether it is paid in full; there is no account activity; the loan was referred to legal for civil action; the individual declared bankruptcy or is deceased; or the loan is resolved).
25. ESDC submits that not all fields were populated in relation to each of the 583,000 borrowers affected by the breach, as not all of these borrowers were the subjects of investigations for the purposes of program eligibility.

CSLP Financial, Business Plan and HR Information

26. Our investigation confirmed that this information refers to documents that capture both CSLP financial and work plan activities that are undertaken on an annual basis in order to assign resources and work for a given fiscal year within the program. Consequently, no personal information was captured in these files.

Employees' Personal Information for Business Continuity Planning

27. Further to paragraph 3 of this Report, ESDC reported to our Office that the external hard drive also contained employee information from a business continuity plan fan out list.

28. We confirmed that a 'fan out list' is used to contact employees in the event of an emergency situation which interrupts their work, such as a building shutdown. The fan out list is an 'evergreen' document; it is updated regularly to ensure that the information is accurate, and to reflect changes in personnel.
29. ESDC confirmed that 250 Learning Branch employees were affected by this incident. The information contained in the fan out list included the employee's first name, last name, home address, home telephone number, and, in some cases, cellular phone number.

ESDC's Actions Following the Incident

30. As part of its submissions to our Office, ESDC provided a comprehensive report of the chronology of actions taken to respond to the incident, including details of the office sweeps and building searches, meetings organized with staff, the communiqués to staff, the preliminary interviews that were conducted with the employee who reported the hard drive missing, and others identified as having access to the hard drive, as well as the steps taken by IITB to locate, scan and review external hard drives located in the building and other locations in the National Capital Region.
31. We highlight the following dates from ESDC's representations:
- On November 5, 2012, the employee's manager was notified of the missing external hard drive and search efforts ensued;

- On November 22, 2012, the Director of the CSLP was notified of the incident and additional search efforts were initiated, including communication with all staff;
 - On November 26, 2012, the Director of the CSLP was advised of the information content on the external hard drive and proceeded to advise senior management of a potential privacy incident;
 - On November 29, 2012, the Security Incident Report was signed off by the Director of the CSLP. The Regional Security Office (RSO) initiated additional searches and sweeps of the office area and building, and also interviewed the employee who reported the incident, and three former employees;
 - On December 6, 2012, following a comprehensive review of the files and folders that were saved to the external hard drive, ESDC determined that the scope of the personal information compromised pertained to over 500,000 clients.
32. On January 4, 2013, ESDC's Special Investigations Unit, Internal Integrity and Security Directorate, was mandated to undertake a formal internal investigation in order to ascertain the circumstances surrounding the loss of the hard drive. ESDC's internal investigation concluded with a report dated February 27, 2013, and a supplementary addendum to the report dated April 9, 2013.
33. As part of its internal investigation, ESDC reported that interviews were conducted with four employees in the CSLP Unit who were identified as part of the working group created to work on the data migration project. These employees were identified as having the hard drive in their possession for the purposes of assisting with the migration project, or having knowledge of its storage location.
34. In addition, the computers of the four identified employees were subject to an IT forensic analysis in order to determine if any external hard drive had been connected to them.
35. Interviews were also conducted with 15 employees working in the same area where the hard drive was reported missing, including two employees currently working in other federal departments.
36. ESDC confirmed that the CSLP area is controlled by an access card system and the access logs for the area were reviewed as part of its investigation.
37. A Canada-wide search was also conducted on ESDC's departmental network to verify if an external hard drive matching the make and model of the missing drive was connected to one of its computers.
38. ESDC's internal investigation established the following facts:
- The initial backup of the information at issue to the external hard drive was conducted in 2011 in the Operational Program Support Division (OPSD);
 - Between January and August 2012, the hard drive was used to conduct sporadic safeguarding (backups) of the information on the T drive by the working group within the CSLP Unit. ESDC established that no files were deleted from the hard drive by the working group members;
 - The IT forensic analysis confirmed that an external hard drive with the same make and model (Seagate GoFlex) was connected in June 2012 to one of the computers searched. ESDC reported that, based on the balance of probabilities, this external hard drive (and its associated serial number) was likely the missing hard drive;

- The IT analysis was inconclusive in relation to two of the computers searched – one employee’s computer was replaced in October 2012 and sent to surplus; and the other computer was reimaged in December 2012, erasing all evidence that a hard drive may have been connected to it;
 - ESDC found no evidence that a Seagate GoFlex external hard drive was ever connected to the fourth computer analyzed during the internal investigation;
 - ESDC also confirmed that the hard drive was left for periods of time (weeks) without being stored in a locked filing cabinet. Even when stored in the cabinet, the cabinet was not always locked and other employees involved in the data migration project were aware of the location of the keys;
 - The external hard drive was last seen by an employee in August 2012, and as previously noted, it was discovered missing on November 5, 2012;
 - The access log report for the period of August 2012 – November 2012 revealed that over 200 different employees had access to the CSLP controlled area. ESDC’s review confirmed that all individuals had approved access;
 - Following multiple searches of the building where the CSLP is located, ESDC found no evidence of a break and enter into the building, or forced attempts to access the cabinet where the hard drive was stored;
 - The information contained on the hard drive was not encrypted and was not protected by a secure password;
 - The procedures outlined in ESDC’s “Departmental Security Policy and Procedures Manual” for handling the information contained on the external hard drive (Protected B), were not followed in relation to storage (where removable media is used to store sensitive information, the media should be stored in a security-approved container); and encryption (sensitive information should be encrypted).
39. ESDC issued a public statement on January 11, 2013 regarding the loss of the external hard drive, providing background information and a timeline of events in relation to the incident on its website.
 40. ESDC submits that, in order to mitigate the impact on those clients affected by the loss of the hard drive, it initiated a public awareness campaign that included press releases, public announcements, and special information on the Department’s website. In addition, ESDC set up a dedicated toll-free information line in order for individuals to verify whether they were affected by the incident, and to obtain additional information regarding the incident. This service was offered to individuals starting on January 14, 2013.
 41. Between January 28, 2013 and February 1, 2013, ESDC sent out notification letters to those clients for which it had current contact information. ESDC advised affected clients of the personal information that was compromised by the loss of the external hard drive, including: Social Insurance Number (SIN), first name, last name, date of birth, home address, telephone number, and student loan balance.

42. In its representations to our Office, ESDC submits that, in the spirit of informing affected individuals as quickly and clearly as possible, the files and fields of information were analyzed and grouped into seven key pieces of personal information, as described above.
43. The notification letters to affected clients also included ESDC's offer for credit protection through an agreement with Equifax.
44. ESDC confirmed that it contracted with Equifax to provide affected clients, upon consent, with free credit and identity protection services. This offer was announced publicly by ESDC on January 25, 2013.
45. ESDC subsequently contracted with the credit bureau TransUnion Canada on June 7, 2013, to offer additional credit protection to clients affected by the incident. ESDC announced this offer to the public on June 28, 2013, stating that individuals who previously provided their consent for the services of Equifax would automatically be included to receive the service from TransUnion Canada.
46. The notation will stay on credit files at TransUnion and Equifax for a period of six years unless affected individuals choose to have it removed. This flag will alert credit grantors that data may have been compromised, and lenders will then take additional steps to verify the person's identity before granting credit or opening or using accounts.
47. ESDC also confirmed that, starting on January 21, 2013, a notation was placed on the SIN record of affected individuals in the Social Insurance Register indicating that the SIN was involved in an incidence of loss. The notation specifies that Service Canada agents must follow an enhanced authentication process prior to issuing another SIN card or modifying information on the SIN record. The authentication process involves the agent asking a series of additional questions and requesting photo identification to validate the identity of the individual. In addition, the SIN transactions on the Social Insurance Register for the affected SINs are reviewed regularly and Service Canada will notify the affected individual immediately of any concern.
48. Although the monitoring function commenced on January 21, 2013, ESDC explained that a retroactive post analysis for all SIN transactions processed during the period from November 5, 2012 to January 18, 2013, was conducted and no anomalies were found. The SIN transactions on the Social Insurance Register (SIR) for the affected SINs continue to be reviewed regularly. To date, ESDC reported that there have been no anomalies detected.
49. SIN monitoring was organized by ESDC until the end of January 2015. A flag will remain on the identified SINs, and as noted above, individuals that request a change to a SIN that was involved in the incident will need to undertake an enhanced authentication process.
50. ESDC reported that the hard drive was not located, and submits that it is unknown whether the disappearance of the hard drive was the result of a human error or malicious intent; however, it submits that, based on analytic reports from Equifax Canada and the Social Insurance Register, it is in a position to indicate that, as of the date of this Report, it has found no evidence of malfeasance connected to the loss of the hard drive.

51. The matter was also referred by ESDC to the Royal Canadian Mounted Police (RCMP) on January 7, 2013 for investigation. It was subsequently reported publicly on August 8, 2013, that the RCMP would not launch a criminal investigation into the matter.

52. ESDC submits that appropriate administrative action has been taken in relation to the incident, in line with Treasury Board Secretariat's "Guidelines for Discipline".

ESDC's Privacy Management Framework

53. ESDC submits that the Department commenced a review of its privacy management framework in 2010, which resulted in the launching of a multi-year privacy renewal initiative.

54. In 2011-2012, ESDC conducted a review of privacy management practices and convened with key stakeholders to inform the development of the Privacy Renewal Action Plan. The first phase of the Action Plan was launched in 2011-2012, which included a privacy risk triage and the drafting of a consolidated Departmental Privacy Code. The new Privacy Code came into force in March 2013.

55. In 2012-2013, four key priorities were identified for the second phase of the Action Plan, including program-led Privacy Action Plans for eight of ESDC's statutory programs; the re-design of the Department's Privacy Impact Assessment (PIA) Process; the launch of a new "Departmental Policy on Privacy Management"; and the implementation of a renewed privacy training and awareness strategy.

Departmental Directives and Protocols

56. On January 14, 2013, ESDC issued new IT Security Guidelines to all staff. The "USB Storage Devices Directive" provides direction that only authorized USB devices are allowed for use on departmental computers. This includes portable hard drives and USB keys.

57. To implement the Directive, all unencrypted USB devices were collected for proper disposal and a limited number of encrypted (password or biometric) are being distributed to employees who regularly work with protected or classified information. Further, ESDC reported that it now regularly scans its corporate network to detect the use of unauthorized USB devices.

58. ESDC also reported that an updated version of its "Information Classification Guide" was reissued on January 15, 2013 to enhance employees' awareness of the requirements for safeguarding protected and classified information.

59. In addition to the new USB Directive, ESDC is conducting a risk assessment of all other mobile devices to identify the risk of loss of personal information. To this end, it has temporarily disabled the ability of employees to write on CDs, DVDs, and other optical media unless a legitimate business requirement is identified and approved.

60. ESDC confirmed that work is ongoing within the department to develop and deliver enhanced integrated training for departmental staff. All employees will be required to undertake mandatory training on the subjects of privacy, security, information technology security, information management and values and ethics. Re-certification will be required every 24 months.

61. The Department is also implementing an 'Engagement Plan' to engage employees on the stewardship of information. To support this Plan, ESDC implemented a portal on the Stewardship of Information in August 2013. The site provides employees with information relating to the management and protection of Departmental information assets, as well as information on the issues of privacy, security, IT security, information management, and values and ethics.

Application

62. In making our determination, we considered sections 3, 6, 7 and 8 of the *Act*.
63. Section 3 of the *Act* defines personal information as information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing: information relating to race, national or ethnic origin, colour, religion, age, marital status, education, medical, criminal or employment history, financial transactions, identifying numbers, fingerprints, blood type, personal opinions, etc.
64. Subsection 6(3) of the *Act* requires that a government institution dispose of personal information under its control in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information.
65. Paragraph 7(a) of the *Act* states that personal information shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose.

66. The *Act* states that personal information can only be disclosed with an individual's consent – Subsection 8(1) – or in accordance with one of the categories of permitted disclosures outlined in subsection 8(2) of the *Act*.

Analysis

67. The personal information contained on the missing external hard drive – for example, name, address, date of birth, SIN – is clearly personal information as defined by section 3 of the *Privacy Act*.
68. Following our analysis of ESDC's policies, in particular, the "Departmental Security Policy and Procedures Manual" (June 2005), the "Policy on Departmental IT Security Management" (December 2010), and the "Departmental Privacy Policy" (last updated in October 2009), we are satisfied that these policies conformed to the requirements of the relevant Treasury Board Secretariat (TBS) policies and guidelines, in particular, the *Policy on Government Security*, the "Operational Security Standard: Management of Information Technology Security (MITS)", and the "Operational Security Standard on Physical Security (OSSPS)".
69. What this means is that we are satisfied that ESDC had in place at the time of the incident the policies commensurate with the requirements demanded by the Government of Canada for the protection of its personal information holdings.
70. Notwithstanding the above, our investigation identified a number of weaknesses in ESDC's control over the personal information identified on the missing hard drive. In our view, the Department failed to translate its own privacy and security policies into meaningful business practices.

71. For ease of reference, we have organized our analysis around four types of controls that the OPC has identified as providing protection against data breaches – what we refer to as the four pillars of sound privacy management.
72. We base these controls on the TBS's *Directive on Privacy Practices* and the *Policy on Government Security*, specifically:
- I. Physical Controls
 - II. Technical Controls
 - III. Administrative controls
 - IV. Personnel Security Controls
- I. Physical Controls**
73. Physical security controls are paramount in ensuring that government information (including personal information), assets and services are protected against compromise. This includes implementing strategies to mitigate the risk of unauthorized access, use or disclosure of personal information.
74. Our investigation established that the CSLP Unit is located in an operational zone, limited to authorized departmental employees. The physical area is controlled by an electronic card access system and is monitored after-hours by a security alarm system. The entrance to the building is monitored by a Commissionaire and visitor access is strictly controlled (sign-in and visitor pass).
75. While base building security is fundamental to safeguarding government employees and assets, physical security strategies must also be in place to protect information and to comply with Government of Canada policies.
76. In line with ESDC's "Departmental Security Policy and Procedures Manual" and the Government of Canada's "Operational Security Standard on Physical Security", protected information, which includes personal information, must be stored in a security-approved container (e.g. approved filing cabinet). It also requires that protected information and valuable assets are properly safeguarded when occupants are away from their workstations for any length of time. Accordingly, keys or other locking features of security containers must also be safeguarded.
77. We highlight that the personal information content on the missing external hard drive is classified at the "Protected B" level, according to the Government of Canada classification standards. TBS states that this applies to sensitive personal, private and business information where compromise could result in grave injury (e.g. loss of reputation, identity theft, etc.).
78. ESDC's "Departmental Security Policy and Procedures Manual" requires that, where removable media is used to store sensitive information, including personal information, the media must be stored in a security-approved container when not in use.
79. Our investigation established that the hard drive was often left unsecured for extended periods of time without being stored in a filing cabinet. Even when stored in the cabinet, the cabinet was not always locked and other employees were aware of the location of the keys.
80. Portable devices are attractive assets and safeguards must be in place to protect the personal information stored on those assets. To this end, we are not satisfied that ESDC had in place robust physical security controls to mitigate the risk of compromise to both the external hard drive and the personal information stored on it.

II. Technical Controls

81. Federal Departments and agencies are required by the *Policy on Government Security* (PGS) to protect government assets and information, including personal information, and are directed to have an IT Security strategy in place to protect information throughout its lifecycle. IT Security refers to the safeguards implemented to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.
82. ESDC's "Departmental Security Policy and Procedures Manual" requires that measures must be established to safeguard personal or other sensitive information throughout its lifecycle. This includes the secure processing, storing, handling, communicating, transmitting and destroying of sensitive information in accordance with departmental security standards, and on the basis of a Threat and Risk Assessment (TRA). Further, it states that personal or other sensitive information must be identified and marked according to its highest level of security.
83. Our investigation determined that removable media (e.g. external hard drives, USB keys, etc.) were not subject to security risk assessment activities at the time of the incident. ESDC did not require that a TRA or a Privacy Impact Assessment (PIA) be conducted in relation to the use of removable media containing personal information. In addition, the missing external hard drive was not marked as required by ESDC's policy.
84. ESDC submits that it annually conducts risk assessment exercises; however, given limited resources, priority was given to higher level threats. Removal media were not identified as a high level threat. In addition, ESDC submits that the use of removable media with desktop or network hardware and software were also not amongst the systems examined at the time of the incident. It indicated that the Department is now proceeding with a progressive certification and accreditation of its systems.
85. ESDC's "Departmental Security Policy and Procedures Manual" also requires that, where removable media is used to store sensitive information, including personal information, the information should be encrypted. Further, ESDC's Security Bulletin entitled "Encryption Requirements" (December 2008), states that, where possible, management should limit situations where employees are required to store protected information, including personal information, on portable media devices. Where unavoidable, it is the employee's responsibility to ensure that the information is encrypted.
86. While ESDC submits that at least two approved procedures were readily available to the users of the external hard drive – 1) the password protection feature; and 2) the use of the Entrust encryption software; – the investigation established that no technological safeguards were implemented to protect the information content on the hard drive in this case.
87. We recognize that ESDC introduced a new "USB Storage Devices Directive" in January 2013 that prohibits the use of unencrypted USB keys and hard drives on departmental computers. To this end, we encourage ESDC to continue with the implementation of this risk management strategy, including regularly scanning network drives to detect unauthorized devices and clearly communicating the new Directive to all employees.

III. Administrative Controls

88. Administrative controls refer to the procedural safeguards implemented for the safe handling of personal information, which includes the enforcement of an institution's policies, directives and processes for the protection of personal information throughout its lifecycle.
89. In order for a federal institution to provide adequate security for personal information under its control, it must have a clear idea of where data is collected and stored. The identification and control of assets, both materiel and information, is a fundamental and critically important aspect of privacy compliance that assists in minimizing the risk of loss or damage to federal assets and information, including personal information.
90. ESDC's "Departmental Security Policy and Procedures Manual" stipulates that the Director or delegate is accountable for the security of all materiel assets listed for the office. Assets Management should be consulted for asset control and inventory requirements.
91. Our review established that, at the time of the incident, there was no comprehensive inventory of the portable devices under the control of the CSLP Unit. In fact, we confirmed that the employees involved in the data migration project were not required to sign for the external hard drive, and the device contained no inventory or tracking number. Moreover, ESDC was unable to conclusively confirm the serial number of the missing hard drive.
92. Departments are not only required to be continually aware of the assets they hold, but must also be aware of their associated sensitivity and criticality. This is the foundation of a risk management philosophy.
93. We are also of the view that there was a lack of effective management and control over the personal information content on the hard drive. In particular, we highlight the following observations:
 - While ESDC submits that the information at issue was initially saved to the hard drive in 2011 by the Operational Program Support Division, the investigation was unable to conclusively establish the exact information content on the hard drive when it was provided to the members of the data migration project (CSLP Unit);
 - Our investigation determined that the members of the data migration project did not have a clear understanding or awareness of the information content on the external hard drive;
 - Our investigation was unable to establish what exact information was backed-up to the hard drive by the members of the data migration team, or the exact information content on the hard drive at the time it was discovered missing.
94. In fact, further to paragraph 17, ESDC submits that there is no way to conclusively determine what was on the hard drive when it was reported missing in November 2012. ESDC created an algorithm in order to scan the network drive to identify files and folders that contained personal information. The information identified during this network scan was reported by ESDC as the information content on the external hard drive.
95. To this end, we are not satisfied that ESDC properly identified or categorized the information according to its sensitivity (i.e. Protected B), or that controls were in place to monitor the security of this information throughout its lifecycle, which includes employee awareness of these sensitivities.

96. Administrative safeguards also refer to the enforcement of an institution's written policies, directives, procedures and processes for the protection of personal information.
97. Further to paragraph 70, while we are satisfied that ESDC had in place at the time of the incident sound policies in relation to the management of its personal information holdings, we are of the view that there is an identifiable gap in the translation of these policies to the day-to-day business operations of the Department.
98. Consequently, we are not satisfied that, at the time of the incident, ESDC had effective controls in place to ensure the management of the information in question throughout its lifecycle.

IV. Personnel Security Controls

99. Personnel security controls refer to a Department's management of its employees – suitability, proper training, supervision and disciplinary procedures.
100. The examination of the trustworthiness and suitability of employees to protect the employer's interests is accomplished by conducting security assessments and reliability checks, which are conditions of employment under the *Public Service Employment Act (PSEA)*.
101. Our investigation confirmed that the employees who had access to the information content on the external hard drive each had a valid security clearance commensurate with the level of information required for their positions.
102. Government of Canada employees are responsible for managing the information they collect, create and use to support the programs and services under which they operate.

103. To accomplish this, employees have a responsibility to apply Government of Canada and Departmental policy instruments (policies, standards and associated procedures). Employees must therefore be provided timely access to training to ensure that they have the necessary knowledge, skills and competencies to effectively carry out their duties.
104. We are not satisfied in this case that the employees who had access to the external hard drive fully understood the privacy risks inherent to the use of a portable device, or the vulnerabilities of the information stored on the device. In fact, it is our view that the employees interviewed during the investigation did not have a clear understanding of the information content on the hard drive at all.
105. Further to paragraphs 70 and 97, it is our view that there is an identifiable gap in the translation of Departmental policies to the day-to-day business operations of the department. To this end, we highlight that there is a lack of employee awareness in the following areas that contributed to vulnerabilities in ESDC's information management practices at the time of the incident:
- Information stewardship – identifying and handling personal information;
 - Security responsibilities – procedures for storing personal information and assets containing personal information;
 - IT controls and responsibilities – implementing safeguards to protect personal information, particularly information stored on portable devices (e.g. encryption);
 - Threats – awareness of the inherent risks associated with the loss or unauthorized access, use or disclosure of personal information.

106. Employee awareness is accomplished through effective management, leadership and the supervision of employees, which support information management practices and mitigate the risks of human error, wrongdoing or negligence. This may include formal direction, follow-ups, monitoring, inspections, and audit controls. There are consequences to non-compliance, and steps must be taken to identify the risks and manage them before they occur.
107. ESDC submits that the IT Security Centre of Excellence, under its IT Security Awareness Program, issues monthly tips and alerts to staff. In addition, the Department sends out periodic reminders to employees on the importance of protecting the personal information of Canadians and the strict procedures to be followed in handling such information. IT Security Awareness Training was also deemed mandatory by ESDC in June 2009 with the approval of the Policy on Departmental IT Security Management.
108. Further to paragraph 60, ESDC submits that work is ongoing to develop and deliver enhanced integrated training for departmental staff. All employees will be required to undertake mandatory training on the subjects of privacy, security, IT security, information management and values and ethics.
109. We encourage ESDC to continue with the establishment of a comprehensive training and awareness program to ensure that employees have the necessary knowledge, skills and competencies to effectively carry out their information management duties.
110. Further to paragraph 52, ESDC submits that appropriate administrative action has been taken in this case. To this end, Departments are authorized to establish standards of discipline and to set penalties, including termination of employment, suspension, demotion to a position at a lower maximum rate of pay, and financial penalties that may be applied for breaches of discipline or misconduct, in line with Treasury Board Secretariat's "Guidelines for Discipline".

Findings

111. The *Privacy Act* requires government institutions to respect the privacy of individuals by properly managing the collection, use, disclosure, retention and disposal of personal information.
112. ESDC regularly collects personal information for purposes of administering the CSLP. It stands to reason that, in order to meet its obligations to ensure that it does not use or disclose personal information in a manner contrary to the *Act*, it is a necessary precondition that ESDC protect the personal information it has collected during its life cycle - from the time of collection until it is destroyed by an approved method.
113. In order to effectively protect the personal information against unauthorized uses and disclosures, government institutions must implement appropriate security safeguards.

114. This notion is supported at the policy level within the federal government. For example, TBS's *Directive on Privacy Practices* calls for limiting access and use of personal information by administrative, technical and physical means to protect personal information, and TBS's *Policy on Government Security* and its related standards establish minimum safeguards to protect and preserve the confidentiality and integrity of government assets, including personal information.
115. ESDC's failure to implement the appropriate safeguards to protect the personal information in question has created a significant risk for unauthorized access, use or disclosure – the very threats that the Government of Canada is entrusted to protect it from. Of great concern is the volume and sensitivity of the personal information contained on the external hard drive – information that could, in the wrong hands, lead to identity theft or fraud.
116. ESDC also has a responsibility to ensure it disposes of personal information in accordance with the requirements of the *Act*, which includes a requirement that the information be disposed in accordance with any directives or guidelines issued by the designated minister (i.e., the President of the Treasury Board).
117. In this regard, the TBS *Directive on Privacy Practices* requires that government institutions dispose of records containing personal information in accordance with the provisions of the *Library and Archives of Canada Act* and according to government security standards.
118. Given that the hard drive in this case is lost, ESDC is not in a position to demonstrate that it complied with these requirements to properly dispose of the personal information contained on the hard drive.
119. Based on the above, we are not satisfied that ESDC has met the requirements of sections 6(3), 7 or 8 of the *Privacy Act* in this case.
120. Accordingly, we have concluded that the matter is **well-founded**.

Recommendations

121. In a letter dated November 4, 2013, our Office provided a Preliminary Report of Findings to ESDC pursuant to subsection 33(2) of the *Privacy Act*. This Report contained details of our investigation and set out the preliminary findings and recommendations of our investigation.
122. To this end, we recommended that ESDC implement a number of security measures to contribute to the prevention of a similar incident, and to help ESDC meet the requirements of the *Act* to protect against unauthorized uses and disclosures of personal information. The recommendations made to ESDC were based on the four types of controls that the OPC has identified as providing protection against privacy breaches, further to paragraph 72 of this Report.
123. In its response to the Preliminary Report of Findings received on December 4, 2013, ESDC accepted our recommendations in full. Set out below are our recommendations and ESDC's response to each of our recommendations.

OPC Recommendation 1

We recommended that ESDC revisit its physical security control practices to ensure that regular monitoring and inspections are incorporated into its security program. This will help to ensure that personal information is stored in approved cabinets when employees are away from their desks for any length of time; that cabinets are locked accordingly; that keys for cabinets are properly safeguarded; and that attractive or valuable assets (i.e. external hard drives, laptops, etc.) containing personal information are properly safeguarded.

ESDC's Response

ESDC submits that it has commenced security sweeps in its buildings, including employee cubicles and offices. ESDC contends that this initiative will raise awareness and help mitigate the potential loss of government assets and information. ESDC is finalizing a plan to conduct security sweeps in all regions.

ESDC highlighted that it is also developing a Departmental Security Framework that sets out the effective management of security responsibilities and imbeds security principles and practices at both the strategic and operational levels. The Framework and associated plans will help to define different types of security requirements, inform improvements to security functions, as well as support security training and awareness.

OPC Recommendation 2

A PIA is a formal process that helps determine whether initiatives involving the use of personal information raise privacy risks, and proposes solutions to eliminate or mitigate privacy risks to an acceptable level. A TRA assists in the determination of IT security requirements and can be short and simple, depending on the sensitivity, criticality and complexity of the program, system or service being assessed. We recommended that ESDC establish protocols to coordinate the identification and categorization of its personal information holdings and assets with departmental PIA and TRA activities in order to mitigate all identified privacy risks.

ESDC's Response

ESDC highlighted that the identification, assessment and mitigation of privacy risks is a key pillar of its Privacy Management Framework. Following the first phase of ESDC's 2011 Privacy Renewal Action Plan which included a series of privacy risk assessments of the Department's major statutory programs and personal information holdings, program-led Privacy Action Plans were developed and launched for the Department's eight statutory programs in 2012 as part of phase two of the Privacy Renewal Action Plan.

In 2012-2013, ESDC submits that it re-engineered its Privacy Impact Assessment (PIA) process to enhance and streamline the Department's privacy risk assessment and mitigation process, and also launched a new strategic planning process to support the implementation of an annual privacy and information security work plan.

ESDC submits that it will continue to support the implementation of a risk-based, proactive approach to privacy management by building on progress achieved to date and identifying and assessing emerging privacy and security risks.

OPC Recommendation 3

We recommended that ESDC complete a comprehensive review of its materiel holdings to ensure that all personal information and assets containing personal information are identified and marked according to the highest appropriate security level (e.g. “Protected B”), in line with ESDC’s “Departmental Security Policy and Procedures Manual”, and Treasury Board’s “Security Organization and Administration Standard” for selecting minimum safeguards to protect information and assets.

ESDC’s Response

ESDC highlighted that it is presently executing an Information Management strategy across all branches and regions which includes the following core elements:

- i. Examination of all repositories to develop an inventory of information assets;*
- ii. Appropriate retention and disposition decisions to ensure that transitory records which are no longer required are disposed of, and records of business value are preserved;*
- iii. Classification of remaining records to the appropriate security level, following the Department’s information classification guide;*

- iv. Appropriate protection, through access rights, encryption, or both, of information that is rated “Protected” or above.*

OPC Recommendation 4

We recommended that portable storage devices only be used as a last resort to store or transfer personal information, and only if it is demonstrably necessary to fulfill a specific and documented purpose. All sensitive or personal information stored on portable devices must be protected by strong technological safeguards, including encryption.

ESDC’s Response

ESDC highlighted that steps have been taken to restrict and manage the use of portable storage devices, including: 1) On January 11, 2013, the “USB Storage Devices Directive” was implemented that restricts the use of portable storage devices to instances where management has validated the need, mandates the use of encrypted (biometric and password) USB keys or hard drives, and imposes consequences for failure to comply; 2) On January 18, 2013, the monitoring of desktop computers for unauthorized use of USB devices began; 3) On May 27, 2013, security software was deployed to block unauthorized use of USB devices; and 4) On June 3, 2013, security software was deployed to block all other portable storage devices, such as optical media (CD/DVD) and floppy disks. Only authorized users can save to such media.

OPC Recommendation 5

We recommended that ESDC establish proper materiel management practices to inventory and monitor all assets that may be used to store or transmit sensitive personal information. This may include affixing a bar code or other inventory measure to enable tracking of the asset. In addition, the relevant asset information (e.g. serial number) must be communicated to the appropriate asset management staff.

ESDC's Response

ESDC confirmed that, as a result of the incident, portable devices are now procured, distributed and managed centrally, and Assistant Deputy Minister (ADM) approval is required to use such devices. In addition, ESDC highlighted that laptops are tagged and tracked by serial number and report to a technical console each time they are connected to ensure proper security software is deployed. Encrypted USB keys and portable hard drives are tracked by serial number – this information is integrated into the software which is used to monitor connections to the Department's network. As a safeguard, devices are attached with a coloured tag that identifies the Department's Service Desk 1-800 number, in the event a device is found. ESDC also confirmed that the Department's Material Management Policy is being updated to reflect how these devices are tracked.

OPC Recommendation 6

We recommended that ESDC incorporate regular security reviews or physical inspections of assets containing personal information to ensure proper safeguards are implemented to protect personal information.

ESDC's Response

ESDC submits that the following efforts will assist the Department in raising awareness among its employees and will enhance mitigation of the potential future loss of government assets and information:

- i. The "Clean Desk Guideline" was shared with all employees in August 2013, to encourage a clean desk practice to prevent the unauthorized disclosure of sensitive information and loss of personal items;*
- ii. Security sweep inspections of employee cubicles and offices have commenced;*
- iii. A compliance validation is included in the approved scope of the Internal Audit on IT Security, whereby individual, portable digital media will be examined to assess controls in the areas of policy management, technical security and operational security. The conduct phase of the audit is proceeding until July 2014.*

OPC Recommendation 7

We recommended that ESDC develop and implement controls to ensure that personal information is managed rigorously throughout its entire lifecycle. This includes establishing controls to manage and track personal information, and ensuring that there is awareness and accountability for the information throughout its lifecycle.

ESDC's Response

ESDC attests that a critical element of its Information Management strategy is ensuring the appropriate classification of records and the appropriate storage of records classified at protected or above. Through proper training, a disciplined process, and regular follow-up, ESDC submits that awareness of the proper handling of sensitive records will remain high.

Effective June 2013, Data Loss Prevention (DLP) software has been deployed which permits routine scanning of information repositories. Advanced algorithms detect when potentially sensitive files are not properly protected, which allows management to take action to ensure the records are more appropriately managed.

ESDC further submits that promoting employee awareness and accountability for personal information throughout the information lifecycle is a key component of its Privacy Renewal Action Plan. ESDC highlighted some of its ongoing efforts, including a privacy awareness week in January 2013; activities organized in all branches and regions between February and June 2013 to directly engage employees on the importance of personal information protection; the launch of a new 'Stewardship of Information' portal to provide employees with information

about roles and responsibilities, policies, tools, and other resources on the subjects of privacy, security, information management, and values and ethics, in August 2013. ESDC will continue to reinforce awareness of employee roles and responsibilities and the risks and threats associated with the protection of personal information through targeted outreach and awareness activities.

OPC Recommendation 8

We recommended that ESDC's training and awareness program include a particular focus on the following:

- Strategies to ensure that all employees understand their roles and responsibilities for the management of personal information through its lifecycle, including identifying and handling personal information;
- The requirements for physical security outlined in ESDC's own "Departmental Security Policy and Procedures Manual" (approved cabinets, locking devices, etc.), including the requirements for the proper operation and safeguarding of attractive or valuable assets that contain personal information (i.e. external hard drives, laptops, etc.);
- The requirements for safeguarding personal information, including IT controls for portable devices (e.g. encryption). Employees that have access to sensitive personal information must be aware of the privacy risks inherent to the use of portable devices, as well as the vulnerabilities of the information that may be stored on these devices (i.e. loss or unauthorized access, use or disclosure of personal information);
- The consequences of not adhering to Departmental security and privacy standards.

ESDC's Response

ESDC highlighted that in April 2013, the Department approved an integrated learning strategy aimed at new and existing employees that consolidates learning in the key areas related to the protection of personal information. As a further measure, all new and existing Departmental employees are required to undertake mandatory testing every two years to ensure ongoing compliance to the functions related to the protection of personal information.

ESDC also submits that when a portable storage device is issued, the employee signs an acknowledgement that they have received the device and understand the provisions for its use.

OPC Recommendation 9

We recommended that participation in training sessions should be mandatory and participation should be documented.

ESDC's Response

As part of its learning policy suite, ESDC submits that the Department approved new mandatory training guidelines that clearly outline the approach, roles and responsibilities for management and employees on the learning requirements relating to the new mandatory Stewardship of Information and Workplace Behaviours Training Program. This training program, which integrates training for privacy, information technology security, information management, security and values and ethics/code of conduct, was approved as a Departmental mandatory learning objective and was launched in September 2013. During this

first phase, the training program was further refined and systems issues were addressed. As a result, the training program was re-launched in February 2014. It is anticipated that all employees will complete the training by August 2014.

All employees will be required to undertake the mandatory training and testing. The Department will be tracking compliance with the mandatory learning objective through a learning management system, and quarterly completion reports will be provided to senior officials. Senior management is accountable for the effective monitoring of employees' attendance regarding the mandatory training, testing and revalidation.

OPC Recommendation 10

We recommended that ESDC incorporate measures to monitor personal information management practices, particularly in those cases where it is necessary to use or transfer personal information to portable storage devices (i.e. external hard drives, laptops, etc.). This may include formal direction, follow-ups, inspections, or audit controls.

ESDC's Response

ESDC submits that the following steps are in place to monitor information management practices with respect to potentially sensitive information:

- *In accordance with the "USB Storage Devices Directive", all USB devices for saving information must be encrypted biometrically or with a password;*

- *Each person who receives an encrypted device signs an acknowledgement of the standard for acceptable use of the device and agreement to submit it for audit at any time. The Internal Audit of IT Security will include a provision for this compliance check;*
- *USB ports are monitored and IT security prepares a weekly report on potentially unauthorized use of USB devices; and*
- *Data Loss Prevention tools are scanning file repositories to identify files which may present a risk.*

Other Observations

124. In our Preliminary Report of Findings, we also offered our observations to ESDC in relation to the Departmental response to the incident – specifically, the immediate actions taken within the Department following the incident, and its notification to the affected individuals.
125. Concerns were raised to our Office by individuals who filed complaints regarding the delay by ESDC to notify affected individuals of the incident. In accordance with Treasury Board’s “Guidelines for Privacy Breaches”, notification to those affected by the incident, particularly in cases where sensitive personal information is compromised, “...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.”
126. In our view, considering the scope of the breach and the mitigation measures that were necessary to be implemented by ESDC following the loss of the external hard drive, we find that the delay in notifying affected individuals in writing was reasonable in the circumstances.

127. We acknowledge in this case that substantial efforts were devoted to searching for the missing external hard drive, including conducting IT forensic analyses; identifying the individuals affected by the incident and confirming mailing information; initiating a public awareness campaign (setting up a call centre, preparing press releases, etc.); coordinating SIN monitoring; arranging an agreement with Equifax for credit protection services; and of course, issuing a public statement on January 11, 2013.
128. Notwithstanding the above, we would like to highlight that that there may have been more personal information compromised as a result of the loss of the hard drive than was reported by ESDC to affected individuals. Further to paragraph 20, ESDC’s representations described the specific fields of information that may have been compromised as a result of the incident.
129. While ESDC submits that these fields of information were grouped into seven key pieces of personal information in order to inform affected individuals as quickly as possible, we failed to see how some of the personal information that was not reported in ESDC’s notification letter to affected individuals – for example, a borrower’s gender, language or marital status – can be grouped into the “seven key pieces of personal information” as ESDC submits.
130. In our view, the combination of certain types of sensitive personal information increases the risks for identity theft, and therefore, it is essential in our view that a complete list of the personal information elements relating to the individual that is thought to have been or potentially been compromised, is included in the notification.

131. Transparency is a key fundamental principle that upholds government accountability. To this end, we remind ESDC of Treasury Board's guidance for reporting and responding to privacy breaches, specifically, the "Guidelines for Privacy Breaches". We also underline the importance of compliance with Treasury Board's *Policy on Privacy Protection* which, as one of its objectives, is meant to enhance effective application of the *Privacy Act* and its Regulations.

132. In its December 4, 2013 response to our Office, we highlight the following comments from ESDC:

- *ESDC submits that the scale and scope of the privacy breach required it to take a number of steps to clearly identify what was missing and who was impacted. Advising Canadians and clients as quickly as possible was of primordial importance in this instance, and as a result, ESDC issued written notices and followed up with written letters to all clients for whom the Department had a valid address.*
- *ESDC contends that waiting to prepare individualized letters containing the specific information that may have been contained on the hard drive would have unnecessarily delayed the notification process. Since the initial notification letters were mailed, clients have contacted the Department requesting confirmation of their specific information that was believed to be contained on the hard drive. The Department has responded to these requests with the exact personal information associated with the particular client making the request.*

- *ESDC further submits that, to date, it has received no indication that any of the personal information potentially stored on the external hard drive has been accessed or used for fraudulent purposes. ESDC submits that it makes this statement following its review of the monitoring of Social Insurance Numbers, as well as in-depth reviews of affected clients' consumer profiles by Equifax, the credit bureau with which the Department has contracted to monitor the credit history of interested individuals affected by this incident.*

Conclusion

133. Our investigation reviewed the physical, technical, administrative, and personnel controls in place at ESDC at the time of the incident – what we refer to as the four pillars of sound privacy management. In our view, these controls should be incorporated into an institution's privacy management framework to protect against data breaches, including the improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information.
134. Our investigation identified a measurable gap in ESDC's implementation of its privacy and security policies in the day-to-day business operations of the Department. This gap resulted in weaknesses in information management controls, physical security controls, and most importantly, the level of employee awareness of Departmental policies and procedures.

135. While we have found ESDC to be in contravention of sections 6(3), 7 or 8 of the *Privacy Act* in this case, the Department has accepted all of our recommendations in full and is in fact well-advanced in the implementation of many of the recommendations identified.
136. Accordingly, we are satisfied that no further action is required by our Office at this time. Nonetheless, we will follow-up with ESDC in one year to confirm its progress in the implementation of our recommendations and its ongoing efforts towards the management of the Department's personal information holdings.
137. We also take this opportunity to highlight that there needs to be a synergy between privacy and security controls to effectively mitigate privacy risks. It is the implementation of these very controls that will assist ESDC to adequately protect the personal information that Canadians entrust to it.
138. It is expected that ESDC will respect the spirit and requirements of the *Privacy Act* – privacy is a fundamental value to Canadians, and it is an essential element in maintaining public trust in government. Therefore, we remind ESDC that it needs to continually be aware of the personal information and assets it holds, and their associated sensitivity and criticality. The protection of personal information must be properly integrated in all Departmental functions, which requires the establishment of a governance structure that has the weight, composition and mandate to effectively ensure implementation of policy instruments.

Additional Information

139. For more information about our Office and the powers of the Privacy Commissioner, please visit us online at www.priv.gc.ca. We also have a number of resources available on our web site that may be of interest to those affected by this incident, including resources about identity theft and fraud.