Audit of the Management of Information of the Canada Student Loans Program (CSLP) – Service Providers

Project No: 6536/04

<u>Project Team</u>

Senior Director:	*B. McNab*
Audit Director:	*W. A. Sanderson*
Team Leader:	*B. Cyr*
Audit Team:	*A. Farley*
	M. Gagnon
	J. Tremblay

<u>APPROVED:</u>

DIRECTOR:	*Benjamin Cyr*	*October 27, 2005*
	Name	Date
DIRECTOR GENERAL:	*Barbara McNab*	*October 27, 2005*
	Name	Date

October 2005

SP-653-10-05E
(également disponible en français)

Paper
ISBN : 0-662-43356-4
Cat. No.: HS28-47/2006E

PDF
ISBN : 0-662-43357-2
Cat. No.: HS28-47/2006E-PDF

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Objective

The objective of this audit is to provide assurance that management of information by the Service Providers is appropriate. Information should be:

- sufficient, reliable, and available in a timely and proper fashion;
- used for program management and accountability; and
- properly collected, used, disclosed, retained and disposed of in compliance with applicable legislation, including the *Privacy Act*, policies and procedures.

Scope

This audit was conducted on site at the Service Providers. These Service Providers are responsible for managing student direct loan accounts on behalf of the Canada Student Loans Program (CSLP). Internal Audit reviewed and analysed the management of information. In accordance with the approved Terms of Reference, only major aspects of the protection of personal information were covered. Also, some criteria have already been partially covered by KPMG's audit reports. Those results were validated and considered for this audit.

Methodology

As per Treasury Board's Internal Audit Guidelines and Professional Internal Audit Standards, assurance was provided through a number of methodologies and tools including:

- interviews;
- analysis of documents;
- on site observations;
- system analysis; and
- data analysis, validated through sampling.

Please refer to the Appendix A – *Audit Objective, Criteria and Methodology*.

Professional Auditing Standards

This internal audit was conducted in accordance with the Treasury Board Policy on Internal Audit and the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing.

Main Findings

- Auditors found that the Service Providers had the information they needed to perform their day-to-day activities and assist them in their decision making process.

- There were also weaknesses with one of the service provider's processes and controls:

  - Disbursement Module System: when a disbursement is made by cheque, it is possible for an employee to make changes to a student's address without any flags being raised. However, the risk is low since most of the disbursements are done through direct deposits.

  - A small number of employees were asked to work on Canada Student Loans files during peak periods without having their Enhanced Reliability Clearance. However, as required under their Statement of Work, employees working on students' files must have this level of clearance.

- The Service Providers do not report to the CSLP on all Service Levels required under their Statement of Work. Therefore, this could cause certain difficulties to the CSLP management to appropriately monitor all activities.

- The handling and protection of personal information is well incorporated in the management framework of both Service Providers.

- Clear retention and disposal guidelines have not yet been developed by the CSLP. This issue should be resolved as soon as possible in order to give clear directives to both Service Providers concerning the retention of personal information.

- Auditors found that some privacy aspects were not fully respected and followed at one of the service provider's premises. For example, in some cubicles, we have observed that personal information had been disposed of in recycling bins. This increases the risk for this type of information to get into the hands of unauthorized individuals.

- Adequate controls were in place regarding the accessibility of personal information.

Audit conclusion and standard Statement of Assurance

Our overall opinion is that the management of information by the Service Providers is appropriate, however, there is room for improvement.

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses of the situations as they existed at the time of the audit against the pre-established criteria. The conclusions are only applicable for the Management of Information of the Service Providers for the Canada Student Loans Program (CSLP).

Recommendation 1:

We recommend that the CSLP's management ensure that the service provider:

- implements a control feature in the Other Information screen section in the Disbursement Module System (key entry 2) in a way that a flag is raised if any information is changed;
- makes changes to the procedures so that the supervisor of the Disbursement area distributes the batches to the employees (key entry 2); and
- permits only those employees who have their Enhanced Reliability Clearance to work on any CSLP file. Furthermore, the CSLP's management should determine the cause of the delays in obtaining the Enhanced Reliability Clearance for the service provider's employees.

Recommendation 2:

We recommend that the CSLP's management review and monitor all Service Levels within the Statement of Work for both Service Providers to ensure the information is reliable.

Recommendation 3:

We recommend that the CSLP's management ensure that the Service Providers report on all Service Levels.

Recommendation 4:

We recommend that the CSLP's management establish clear guidelines for the retention period with both Service Providers and incorporate these guidelines in their contracts. We also recommend that the CSLP's management ensure that one of the service providers makes the necessary changes on its document once these guidelines have been clarified.

Recommendation 5:

We recommend that the CSLP's management ensure that the service provider keeps all their fax machines in secure areas and separate from large quantities of papers.

Recommendation 6:

We recommend that the CSLP's management remind the service provider to ensure that all employees use the shredding security consoles on their premises to dispose of clients' personal documents.

1. BACKGROUND

This assurance audit examined how the Service Providers were managing the information of the Canada Student Loans Program. They have been operating as the National Student Loans Service Centre (NSLSC). This audit was identified in the Internal Audit Annual Plan based on a cyclical coverage.

The Canada Student Loans Program (CSLP)'s mandate is to promote accessibility to post-secondary education by providing loans or grants to qualified students based on their financial need, regardless of the province or territory in which they reside.

Between 1964 and 1995, financial institutions provided loans to post-secondary students who were approved to receive financial assistance. The financial institutions also administered the loan repayment process. In return, the Government of Canada guaranteed each Canada student loan that was issued by reimbursing the financial institution the full amount that went into default. From 1995 to 2000, the federal government developed a formalized "risk-shared" agreement, whereby the institutions assumed the risk of defaulted loans in return for a fixed payment.

Since the beginning of August 2000, the government has provided a regime of direct loans governed by the *Canada Student Financial Assistance Act* under which it finances the loans and bears the full risk. One of the service providers administers loans issued to students attending public educational institutions, whereas the other one administers those issued to students attending private educational institutions. The two Service Providers are responsible for managing students' direct loan accounts on behalf of the CSLP.

Under the new direct loans model, the goal of the CSLP is to improve its accountability by regularly measuring program performance and borrower surveys, thereby providing improved service and information to students. Four main objectives were established for the CSLP:

- maintain the government's commitment to accessibility;
- make the loan experience a positive one;
- increase awareness; and
- ensure performance, integrity and accountability.

Objectives

The objective of this audit is to provide assurance that management of information by the Service Providers is appropriate. Information should be:

- sufficient, reliable, and available in a timely and proper fashion;
- used for program management and accountability; and

- properly collected, used, disclosed, retained and disposed of in compliance with applicable legislation, including the *Privacy Act*, policies and procedures.

Scope

This audit was conducted at the Service Providers' sites. Internal Audit reviewed and analysed the management of information. Auditors only examined the information that was produced and received by the Service Providers. In accordance with the approved Terms of Reference, only major aspects of the protection of personal information were covered.

Also, some criteria were partially covered by KPMG audit reports and their results were validated and taken into consideration for this present audit. KPMG's role is to examine the accompanying description of the stated internal control objectives of the student loans processes for both Service Providers and the control procedures designed to achieve those objectives. They also perform tests of the effectiveness of those control procedures on a yearly basis.

Methodology

As per Treasury Board's Internal Audit Guidelines and Professional Internal Audit Standards, assurance was provided through a number of methodologies and tools including:

- interviews;
- analysis of documents;
- on site observations;
- system analysis; and
- data analysis, validated through sampling.

This audit was conducted in accordance with both the Treasury Board Policy on Internal Audit and the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing.

2. AUDIT FINDINGS

2.1 Audit Objective

The objective of this audit is to provide assurance that management of information by the Service Providers is appropriate. Information should be:

- sufficient, reliable, and available in a timely and proper fashion;
- used for program management and accountability; and
- properly collected, used, disclosed, retained and disposed of in compliance with applicable legislation, including the *Privacy Act*, policies and procedures.

2.2 Findings by criterion

Criterion 1

Information is available to allow management to report confidently on their achievements, and make informed decisions that allow for continual improvement.

Both Service Providers have met this criterion.

The management teams of both Service Providers have told us that they receive all the information they need in a timely manner from all stakeholders. Most of the electronic information exchanged between the Service Providers and stakeholders are data files as opposed to reports, therefore the auditors could not verify the detailed content of the electronic data. We noted that some reports described the contents of the document, for instance terminology lists or formulas.

There are weekly conference calls between the Service Providers and the Canada Student Loans Program (CSLP) to discuss operational results and evolving issues.

The Service Providers were not initially involved in the development of CSLP’s performance measures (Service Levels as described in the Statement of Work). Ever since the contracts were granted, both Service Providers have been consulted prior to any additions or modifications to these Service Levels.

Criterion 2

Processes and controls are in place to ensure the reliability of the information.

This criterion has not been fully met by both Service Providers.

Some issues were found on site at both Service Providers. Even though there is a double entry feature in both of their systems, we have observed some weaknesses within one of the service provider’s Disbursement Module System.

A double entry function is a control in itself. One individual enters all the information in the system (key entry 1) and then a second individual must re-key some of the information and review the rest of the data (key entry 2). For five out of the nine provinces, including the Integrated Provinces, most of the information is already entered into the system, reducing the processing time for key entry 1.

At one of the service providers, we noted that its Case System for disbursements had the necessary controls to ensure the information is reliable. For example, employees do not have the ability to choose which file they will be working on. The system automatically brings the next queued file on an employee's screen. In addition, the employee must process the file that appears on the screen before being able to process the next file. Finally, when the key entry 1 and key entry 2 do not match, the file will return to the queue and the process will continue until the two employees' entries match. All these procedures reduce the risk of fraud or errors.

The Case System at one of the service providers uses imaging technology for incoming student documentation. With no paper in the process, there is a reduced risk of losing documents.

At one of the service providers, there is also a double-entry feature in its Disbursement Module System. The key entry 1 will enter all the information needed in a student file. The key entry 2 will then have to re-enter information in the *Double-Entry* screen section (Student Loan Agreement, Banking and Loan Information). The key entry 2 must also review the screen section named *Other Information* (Student, Personal, Loan and Next of Kin Information).

In the *Double-Entry* screen section, if the second entry differs from the first one, a flag is raised and the manager has to approve the modification for the process to continue. However, in the *Other Information* screen section, the information may be changed without any flags being raised. Even though there are risks for internal fraud, mainly if the second employee changes the address of the student when the disbursement is made by cheque, we consider this to be a low risk since students would likely let the Service Provider know if they do not receive their cheque.

In addition, at one of the service providers the individual who does the key entry 1 assigns their batch of files to the person doing key entry 2, creating a potential risk of collusion and fraud.

At the service provider there is an issue regarding the Enhanced Reliability Clearance. The CSLP requires that all employees working on a student's file must have this level of clearance. We have been informed that it can take months for employees to obtain their clearances whereas it takes only one week for the other service provider. Furthermore, employees from other areas could be asked to work on the CSLP files during peak periods even though they have not received their Enhanced Reliability Clearance. We have been informed that Public Works and Government Services Canada is the cause for the delays.

Recommendation 1:

We recommend that CSLP's management ensure that the service provider:

- implements a control feature in the *Other Information* screen section in the Disbursement Module System (key entry 2) so that a flag is raised if any information is changed;
- makes changes to the procedures so that the supervisor of the Disbursement area distributes the batches to the employees (key entry 2); and
- permits only those employees who have their Enhanced Reliability Clearance to work on any CSLP file. Furthermore, the CSLP's management should determine the cause of the delays in obtaining the Enhanced Reliability Clearance for the service provider's employees.

Finally, none of the Service Providers have procedures or documents they can use to establish performance measures. After analyzing the reports the Service Providers sent to the CSLP, we found that not all Service Levels are reported on. Although we were told that external auditors continuously review their Service Levels, we found that the work is mostly comprised of financial data and does not address all the Service Levels.

Recommendation 2:

We recommend that the CSLP's management review and monitor all Service Levels within the Statement of Work for both Service Providers to ensure the information is reliable.

Criterion 3

A reporting structure is in place, which enables the information to be effectively conveyed to management and other users of the information.

Generally, the two service providers have met this criterion.

Most of the electronic information exchanged between the Service Providers and stakeholders are data files, as opposed to reports. A specific group at the Service Providers' offices receives information sent through Government Telecommunications and Informatics Services (GTIS). They can retrieve and transfer the data into the system, but they cannot open or modify a file.

Regarding performance results, all the CSLP Service Levels required in the Statement of Work (and the first amendment to the contract) should be reported on. A number of performance measures from the reports of the Service Providers cannot be matched to the CSLP Service Levels.

Recommendation 3:

We recommend that the CSLP's management ensure that the Service Providers report on all Service Levels.

Criterion 4

Handling and protection of personal information are incorporated in the management framework.

In general, both Service Providers have met this criterion.

The authorities for collecting and using personal information are stated in the contracts and the related Statement of Work for both Service Providers. However, when we asked them under which authorities they could collect and use personal information, we were told that it was through the *Privacy Act* and also due to the fact that they had received their Enhanced Reliability Clearance.

Both managers and employees at the service providers have stated that they are aware of their accountability for the protection and proper use of personal information. Moreover, employees have to sign an agreement to that effect.

Many policies and procedures on these issues are available at both Service Providers. The employees receive training on the collection and proper use of personal information. They also receive information at staff meetings, and in e-mails or news bulletins. At one of the service providers, we observed privacy awareness posters and screen savers that provide tips about privacy.

KPMG conducts the audit report 5900 annually. This audit partially covers the handling and protection of personal information. Both Service Providers have informed us that they also conduct control self-assessments regularly to identify risks and control weaknesses.

Criterion 5

Retention, protection and disposal of personal information meet appropriate legislation, policies and guidelines.

This criterion has not been fully met by one of the service providers.

We obtained a document from the Records Management at National Headquarters stating that the CSLP's hard copy files should be retained for 35 years, but there is no reference to imaged documents. The Service Providers are not aware that such a policy exists. We were informed that one of the service providers retains all documents because there are no relevant policies or guidelines. On the other hand, the other service provider has developed its own retention period guideline which states that "Student loan documentation – Canada and provincial student loans" will be kept for seven years. These guidelines contain discrepancies compared to the Headquarters document.

Recommendation 4:

We recommend that the CSLP's management establishes clear guidelines for the retention period with both Service Providers and incorporate these guidelines in their contracts. We also recommend that the CSLP's management ensure that the service provider makes the necessary changes on its document once these guidelines have been clarified.

Both Service Providers are waiting for the CSLP to develop a policy on the disposal of documents; therefore they do not destroy any student files. As a practice, they keep the files in a secure room before archiving them to Iron Mountain, a service for storing and managing records. A third party shreds internal papers at both service providers.

In respect to the safety of media containing personal information, we conclude that overall, they are well protected and accessible only to authorized persons. Only Information Technology personnel have access to the electronic databases and to the servers at the two companies, and these are kept in a secure room. The backup tapes are not kept at either site to further ensure the information is secure.

Regarding paper documents, we saw that the files are being kept in a secure room, though there are some differences between Service Providers. One of the service providers keeps their files in a room that is locked all day and is accessible only by the mailroom employees. The fax machines are locked in this room to keep the incoming information safe. At the second service provider, we observed that the mailroom is locked only at the end of the day and it is easy for employees to access the room. Also, the fax machines are located in different areas where there are large quantities of papers. This increases the risk that a fax will be misplaced or lost. We were told that, once, a student's fax had been lost.

Recommendation 5:

We recommend that the CSLP's management ensure that the service provider keeps all their fax machines in secure areas and separate from large quantities of papers.

We also noticed in some instances at the service provider that papers and printouts containing personal information such as the name, address, and Social Insurance Number (SIN) of clients were put in recycling bins instead of using the shredding security consoles.

Recommendation 6:

We recommend that the CSLP's management remind the service provider to ensure that all employees use the shredding security consoles on their premises to dispose of clients' personal documents.

Criterion 6

Personal information is accessed only by authorized persons.

Both Service Providers have met this criterion.

After analyzing documents and conducting interviews, we conclude that there are adequate and effective internal controls in both offices to ensure that only authorized individuals can request or modify an employee’s system access. One of the service providers reviews these profiles monthly, which is a good practice in our opinion. The second one conducts a review of their employees’ profiles twice a year. This type of control ensures that only authorized employees have access to personal information and to the screens required to do their jobs.

We have noted that the ClientStar System at one of the service providers and the Student Loan System at the second one have audit trails capabilities. However, neither Service Provider utilizes this function. They would only do so if there was a suspicion of wrongdoing or if an anomaly was to appear on one of their reports. To go one step further, the service provider also produces a violation report that indicates whether an employee has attempted to access an area in the system that is not specified in that individual’s system profile. Two employees are then responsible for reviewing the report and doing a follow-up with the employee in question, requesting an explanation as to the reason for the attempt. The service provider expects to have an audit trail viewer in place by the end of 2005.

Even though documents containing personal information do not have “Protected B” written on them, managers and employees from both Service Providers have indicated that they are aware of their accountability and treat each document in a professional manner. There are frequent reminders of the proper handling of personal information through staff meetings, policies, procedures, posters and training, to name a few.

The service providers both have measures in place should there be a security violation or in the event that personal information is disclosed. The first one hasn’t had any such incident. However, at the second service provider, we were informed that this type of situation has occurred in the past. For example, a student received documents in the mail belonging to another student. Following that incident, a quality assurance group was created to review all outgoing correspondence.

3. CONCLUSION

Our overall opinion is that while the Service Providers are managing information appropriately, there is still some room for improvement.

Therefore, we conclude that:

- The Service Providers had the information they needed to perform their day-to-day activities and assist them in their decision making process.
- There were weaknesses with some of one of the service provider's processes and controls:
  - Disbursement Module System: when a disbursement is made by cheque, it is possible for an employee to make changes to a student's address without any flags being raised. However, the risk is low since most of the disbursements are done through direct deposits.
  - A small number of employees were asked to work on Canada Student Loans files during peak periods without having their Enhanced Reliability Clearance. However, as required under their Statement of Work, employees working on students' files must have this level of clearance.
- The Service Providers do not report to the Canada Student Loans Program (CSLP) on all Service Levels required under their Statement of Work. Therefore, this could cause certain difficulties to the CSLP management to appropriately monitor all activities.
- The handling and protection of personal information is well incorporated in the management framework of both Service Providers.
- Clear retention and disposal guidelines have not yet been developed by the CSLP. This issue should be resolved as soon as possible in order to give clear directives to both Service Providers concerning the retention period.
- Some privacy aspects were not fully respected and followed at one of the service provider's premises. For example, in some cubicles, we have observed that personal information had been disposed of in recycling bins. This increases the risk for this type of information to get into the hands of unauthorized individuals.
- Adequate controls were in place regarding the accessibility of personal information.

Statement of Assurance

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses of the situations as they existed at the time of the audit against the pre-established criteria. The conclusions are only applicable for the Management of Information of the Canada Student Loans Program (CSLP).

This internal audit was conducted in accordance with the Treasury Board Policy on Internal Audit and the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing.

APPENDIX A

Audit Objective, Criteria and Methodology

The objective of this audit is to provide assurance that management of information by the Service Providers is appropriate. Information should be:

- sufficient, reliable, and available in a timely and proper fashion;
- used for program management and accountability; and
- properly collected, used, disclosed, retained and disposed of in compliance with applicable legislation, including the *Privacy Act*, policies and procedures.

Audit Criteria

The criteria are divided in two categories: Management of Information and Privacy.

Management of Information

1. *Information is available to allow management to report confidently on their achievements and make informed decisions that allow for continual improvement.*

1.1 Management information received from stakeholders reflects the needs of the Service Providers.

1.1.1 The information received from the Provinces allows the Service Providers to carry out their day-to-day activities.

1.1.2 The information received from the Canada Student Loans Program (CSLP) allows the Services Providers to carry out their day-to-day activities.

1.1.3 The information received from Educational Institutions (EI) allows the Service Providers to carry out their day-to-day activities.

1.2 Information received by the Service Providers and produced by them is clearly defined to ensure they can be interpreted consistently between stakeholders (Provinces, EI and the CSLP) and internally:

- terminology, and
- figures.

1.3 The Services Providers were consulted with and involved in the development of the performance measures they have to report on to the CSLP.

2. *Processes and controls are in place to ensure the reliability of the information.*

   2.1 Data are protected from unauthorized access and/or modification.

   2.2 Information is updated promptly when obtained and a record of the source of information used to modify information is kept.

   2.3 Source data are precisely defined for each performance measure.

3. *A reporting structure is in place, which enables the information to be effectively conveyed to management and other users of the information.*

   3.1 The reporting structure of information provides:

      3.1.1 consistency across the stakeholders (Provinces and the CSLP); and

      3.1.2 timeliness to carry out day-to-day activities (the CSLP, Provinces and EI).

   3.2 Information is reported to the intended user.

   3.3 Results are reported against established CSLP service standards.

Privacy

4. *Handling and protection of personal information are incorporated in the management framework.*

   4.1 Authorities for the collection and use of personal information are properly defined, documented, disclosed, and related to the CSLP.

   4.2 Accountability for the protection and proper use of personal information is defined and documented.

   4.3 Policies, guidelines and procedures on the handling and protection of personal information are available.

   4.4 Personnel have been informed and/or trained on the handling and protection of personal information.

   4.5 Audit, monitoring, risk and control assessments on the handling and protection of personal information are performed on a regular basis.

5. *Retention, protection and disposal of personal information meet appropriate legislations, policies and guidelines.*

   5.1 Personal information is scheduled for retention and is disposed of in accordance with the appropriate legislations, policies and guidelines.

   5.2 Electronic databases containing personal information, tapes and other physical media containing personal information are protected and kept in secure places that are accessible only to authorized persons.

6. *Personal information is accessed only by authorized persons.*

   6.1 Adequate and effective internal controls are in place to provide assurance that:

      6.1.1 requests to provide or modify access to personal information originate from an authorized person; and

      6.1.2 access profile of an employee whose status, position or function has changed is modified, suspended or removed if required.

   6.2 Viewing of personal information is monitored regularly to detect unauthorized or unjustified access through audit trails or other appropriate means of controls.

   6.3 Material containing personal information is identified as "Protected" and handled in accordance with the appropriate legislation, regulations and policies.

   6.4 Procedures exist to handle security violations or disclosure of personal information (voluntary or involuntary).

Methodology

As per Treasury Board's Internal Audit Guidelines and Professional Internal Audit Standards, assurance was provided through a number of methodologies and tools including:

- interviews;
- analysis of documents;
- on site observations;
- system analysis; and
- data analysis, validated through sampling.

APPENDIX B

MANAGEMENT ACTION PLAN

Internal Audit Recommendations	Management Plan Action(s) to be undertaken	Planned Completion Date	Responsibility Title & RC. Number
1. We recommend that CSLP's Program Management ensure that the service provider's Management: a. incorporate a control feature in the *Other Information* screen section in the Disbursement Module System (key entry 2) in a way that a flag is raised if any information is changed;	a) This observation was also addressed in KPMG Audit Report for 2004-2005. CSLP has discussed this with the service provider's Management and was informed that some compensatory controls are in place. The controls that are in place include weekly and monthly reviews of reports that look at single bank accounts for multiple borrowers and confirm with borrowers that the correct account is being used, all bank account changes are keyed twice by two different people, complete documentation of the request for the change is maintained for audit purposes. CSLP will follow-up during the monitoring activities in 2005-2006. In addition CSLP will also follow-up with the Service Provider to investigate including another flag on their system to highlight "other information" that may be changed and determine a timeframe for implementation.	Completed	DG, CSLP RC 7460
b. have the supervisor of the Disbursement area distribute the batches to the employees (key entry 2); and	b) CSLP will issue a directive for the service provider to comply with this action and will follow up to ensure that this is occurring.	Completed	DG, CSLP RC 7460

Internal Audit Recommendations	Management Plan Action(s) to be undertaken	Planned Completion Date	Responsibility Title & RC. Number
c. not permit employees who do not have their Enhanced Reliability Clearance to work on any CSLP file. CSLP's Management should investigate with all parties involved to determine the cause of the delays in obtaining the Enhanced Reliability Clearance for the service provider's employees.	c) CSLP has discussed this issue with the contracting agency PWGSC to assess whether there have been unreasonable delays in processing the security clearances. PWGSC advises that the timeframes for security clearance of employees typically takes about 3 months, with the exception of clearance for individuals who have been in Canada for less than one year, where contact must be made with the Country of Origin. There is no difference in the handling of security clearance requests between the Service Providers and there have been no unanticipated delays in processing. CSLP will work with PWGSC to ensure that the SP complies with the requirements in the contract with respect to the security clearance of anyone handling CSLP information. PWGSC will resend a message to the service provider reinforcing requirements. Note: Security and privacy issues as well as enhanced audit controls have been incorporated in the RFP for a new service provider.	Completed	DG, CSLP RC 7460
2. We recommend that CSLP's Program Management ensure that all Service Levels within the Service Providers' Statement of Work are reviewed and monitored to ensure the reliability of the information.	SPs provide weekly and monthly reports on the service standards. Program Management reviews all reporting that is done on service standards on an ongoing basis. Note: Criteria contained in RFP for a new SP contains specific service standards and financial penalties if standards are not met.	Ongoing	DG, CSLP RC 7460
3. We recommend that CSLP's Program Management ensure that the Service Providers report on all Service Levels.	CSLP's Program Management will review both the statement of work and monthly reports provided by the SPs to ensure they are reporting on all service standards.	Ongoing	DG, CSLP RC 7460

Internal Audit Recommendations	Management Plan Action(s) to be undertaken	Planned Completion Date	Responsibility Title & RC. Number
4. We recommend that CSLP's Program Management establish clear guidelines for retention period with both Service Providers. These guidelines should be incorporated in their contract. We also recommend that CSLP's Program Management ensure that the service provider make the necessary changes on their documents once clarification has been made.	CSLP will send a directive to both Service Providers, in writing, that no destruction of documents must take place. CSLP will request that the service provider make the adjustment to their policy to reflect that no documents are to be destroyed.	Completed	DG, CSLP RC 7460
	Since CSLP is in a reprocurement process to identify a new Service Provider, guidelines will be developed to coincide with the award of the new contract.	Completed	
5. We recommend that CSLP's Program Management ensure that the service provider keep all their fax machines in secure areas and separately from where there are large quantities of papers.	CSLP's Program Management has contacted the contracting agency PWGSC to discuss proposed changes given they have recently completed a security review. The PWGSC review, in August 2005, found that there were no significant issues related to security issues and fax machines as per the security requirements that were contained in the contract with the Service Providers. CSLP will follow up with the service provider to explore separation of the fax machines from other quantities of paper. Note: Security and privacy issues have been incorporated in the RFP for a new SP.	Completed	DG, CSLP RC 7460
6. We recommend that CSLP's Program Management remind the service provider to ensure that all employees use the shred-it security consoles on their premises to dispose of any clients' personal documentation.	CSLP'S Program Management will notify the service provider and re-iterate this message. Note: Security and privacy issues have been incorporated in the RFP for a new SP. A Risk Management Plan with regular updates is also a requirement for the future SP contract.	Completed	DG, CSLP RC 7460