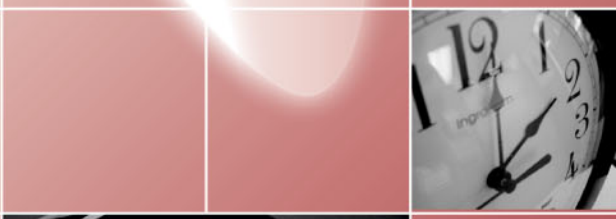
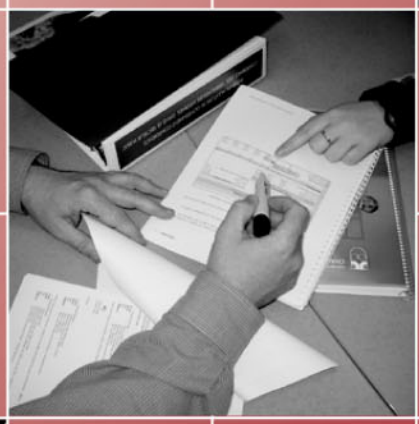
Internal Audit Services

Audit of Management of Personal Information





Government of Canada / Gouvernement du Canada

Human Resources and Skills Development Canada / Ressources humaines et Développement des compétences Canada

Social Development Canada / Développement social Canada

Canada

SP-603-07-04E

Audit of Management of Personal Information

Project No: 6562/02

Project Team

Director General:	*J.K. Martin*
Audit Director:	*G. Duclos*
Team Leader:	*S. Auguste*
Audit Team:	*J. Clément*
	M. Gagnon
	K. Gourlay
	G. Lavergne
	J. Levesque
	S. Malichanh
	A. Markowitz
	C. Tremblay

APPROVED:

DIRECTOR:	*Gilles Duclos*	*July 14, 2004*
	Name	Date
DIRECTOR GENERAL:	*James K. Martin*	*July 15, 2004*
	Name	Date

May 2004

SP-603-07-04E
(également disponible en français)

Paper
ISBN : 0-662-37747-8
Cat. No.: HS3-1/603-07-04E

PDF
ISBN : 0-662-37748-6
Cat. No.: HS3-1/603-07-04E-PDF

HTML
ISBN : 0-662-37749-4
Cat. No.: HS3-1/603-07-04E-HTML

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This audit was initiated in Human Resources Development Canada (HRDC), which has since been reorganized into two new departments—Human Resources and Skills Development Canada (HRSDC), and Social Development Canada (SDC). The acronyms HRSDC or SDC are used in this report when the findings or recommendations apply to only one of the two new departments, and HRSDC/SDC is used when they apply to both. HRSDC/SDC is also used to designate the former department.

The purpose of this audit is to provide assurance that the management of personal information within HRSDC/SDC is in compliance with the *Privacy Act*, particularly *Sections 4 to 8* (commonly referred to as the *Code of Fair Information Practices*) and that the use, disclosure, retention and disposal of personal information meets Treasury Board Secretariat (TBS) and Departmental policies.

The nationwide audit field work was conducted from April to December 2003. It focused on personal information received from the Canada Revenue Agency (CRA, previously known as Canada Customs and Revenue Agency—CCRA) and used by Employment Insurance (EI), Income Security Programs (ISP), Financial Administrative Services-Departmental Accounts Receivable System (FAS–DARS) and Strategic Policy (SP). When appropriate, the audit also included personal information collected by HRSDC/SDC or received from other sources.

The **scope** of the audit was based on the following business objectives:

- Handling and protection of personal information is incorporated in the Departmental management framework;
- Retention, protection and disposal of personal information meets Government Security Policies;
- Personal information is accessed only by authorized persons and used for the purpose for which it was collected;
- Personal information is disclosed in compliance with the *Privacy Act* and other applicable legislation, regulations, policies and agreements;
- Information on the nature and use of personal information is available to the public;
- Individuals have access to their own personal information and procedures are in place to handle complaints.

The criteria associated with these objectives are listed in Appendix A.

Future audits will cover the following aspects of the management of personal information:

- The exchange of personal information with other organizations, departments or levels of government under agreements or Memoranda of Understanding (MOU);
- The collection, handling and protection by HRSDC/SDC of personal information about its own employees;

- The collection of personal information about applicants and clients for the administration of HRSDC/SDC programs.

Methodology

The audit team collected evidence by:

- Reviewing documented policies, procedures and initiatives;
- Interviewing key policy and operational staff and management at NHQ and RHQ;
- Interviewing management and operational staff in the offices visited;
- Analysing actual procedures and controls;
- Testing and observation of the effectiveness of controls.

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

Main Findings and Conclusions of Phase I of the Audit

In this report, "Privacy" is used as a generic term to designate the general management of personal information and the legislative and administrative framework that supports it.

Personal information is defined as information that is or can be related to an identifiable individual.

Confidentiality is the attribute of personal or non-personal information that should only be seen by persons with a right and a legitimate reason to do so. Confidentiality underpins the notions of "need to know" and "browsing" used in this report.

In the opinion of the auditors, awareness of the responsibility and accountability for privacy is increasing in HRSDC/SDC. Three new committees have been created to provide general direction and guidance on privacy issues:

- Privacy Management Framework Steering Committee (PMFSC);
- Databank Review Committee (DRC);
- Information Technology Security Governance Committee (ITSGC).

A draft Accountability Framework for the handling of personal information is being developed. Once completed, it should be communicated and implemented at all levels taking into account the interrelations and the sharing of personal information between the two departments.

Policies and procedures on privacy and security are available on the intranet and internet. Employees are informed of policies and procedures. The policies and procedures that combine security and privacy should be reviewed to ensure that the privacy is adequately and sufficiently covered.

The agreement signed by teleworkers should be standardized to ensure that the clauses dealing with the confidentiality of personal information cover the applicable policies and procedures. Board of Referees members should be subject to a similar agreement.

Training dealing specifically with privacy has been given to Privacy Coordinators. Most employees involved in the handling or disclosure of personal information have received various degrees of privacy-related training and information. To ensure that all employees receive timely and adequate training and information on the use and protection of personal information in their area of activities, a national strategic communication and training plan should be developed.

Management should ensure that those who give or get access to personal information know and understand the nature and application of the "need-to-know" principle and the consequences of violations such as "browsing" and unlawful disclosures.

Personal information is generally retained for the prescribed time before it is destroyed or archived. When material that contains personal information on Departmental clients or other individuals is shipped or destroyed using contracted companies, the contract should specify the responsibility of the contracted firm to protect the confidentiality of the information while this information is under its control. Complete social insurance numbers should not be written on boxes that are shipped out of the Department.

Access to client files and tapes containing personal information is restricted and controlled but the degree of protection against unauthorized access varies between Regions and Programs. The physical protection against unauthorized access or withdrawal of printed material containing personal information varies at each location where documents containing personal information are kept, so individual risk and control assessments should be conducted for these locations.

Employees are generally aware of the rules for amending personal information but clarification is needed regarding the rules and procedures for recording the source and the reason for changes to personal information and for keeping evidence documents.

The various steps in the attribution, maintenance and suppression of User ID[1] should be reviewed to ensure that the accountability and responsibility for User IDs is clearly defined, understood and accepted.

A test to provide assurance that existing User IDs limit access to the personal information required by the user to perform his/her legitimate duties had to be postponed. Conditions that will allow the effective and efficient completion of the test should be established as soon as possible.

PROTECTED

[1] User ID is defined in section 3.2.2

PROTECTED

The Guide on the classification and handling of documents containing personal information should be supplemented with practical guidance for the most frequently used paper and electronic documents containing personal information. Internal controls should be put in place to ensure that protected material is identified and handled according to its classification.

The process to be followed by managers and employees who become aware of a possible privacy violation should be clarified and communicated.

The nature and sensitivity of the information disclosed should be taken into account in the distinction between formal and informal disclosure and the rules for documenting the disclosure should be reviewed.

Employees generally understand their responsibility regarding the disclosure of personal information (verification of identity or delegation and disclosure exemptions) but the rules could be clarified on documenting informal requests for disclosure of personal information in the client's file.

Information about the nature and use of personal information is available to the public through Info Source and clients are informed of their right of access to the contents of their file. Mechanisms to handle privacy related complaints are in place in all Regions visited.

Overall Opinion

Based on our audit work, it is our opinion that important progress has been and is continuing to be made in the management of personal information.

Nevertheless, further improvements are required per our recommendations.

Management has developed an appropriate action plan (Appendix B) to address these recommendations. Its successful completion, especially regarding recommendations 9 to 12, should put in place all the expected controls for the appropriate management of personal information within HRSDC and SDC.

In our professional judgment, appropriate audit procedures have been followed and sufficient evidence has been gathered to support the conclusions contained in this report. The conclusions are based on the situation that existed at the time of the audit against the audit criteria. The conclusions apply only to the management of personal information activities examined.

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.

Overall Management's response

The Director General, Privacy, together with the Privacy Coordinators for HRSDC and SDC, and Directors General from several branches, have reviewed the Audit of Management of Personal Information and collaborated on the preparation of its accompanying management action plan.

The concern that Canadians express for their privacy continues to increase, and the broad availability of integrated service offerings, often through new electronic channels, is one contributing factor. Canadians want assurance that their personal information is being carefully managed within well-defined parameters. The Privacy Act and related program authorities set out our obligations to protect personal information and to ensure its appropriate collection, use and disclosure. These legislative authorities are complemented with policies, procedures and tools that have been the subject of this review.

The internal audit and management action plan represent a key step in the ongoing implementation of the award-winning Privacy Management Framework (PMF). The PMF, and its four pillars of Strategic Planning and Governance, Risk Management, Cultural Change, and Assurance of Compliance, are focusing departmental attention onto privacy matters. Considerable progress has been made and the Departments have been recognized for their initiative.

Together, the PMF and this audit serve to demonstrate how we uphold our obligation to protect the personal information of Canadians. For the past two years HRDC has recognized Privacy as a strategic corporate priority under the goal of Service Excellence. This is explicit recognition, at the highest departmental level, of the importance of privacy to Canadians and their expectations of government to protect it. Both HRSDC and SDC are expected to continue this commitment to the effective management of personal information and incorporate it as an intrinsic component of their respective cultures. As the audit has clearly demonstrated, the effective management of personal information is no different than that of any other strategic asset. This is why controls are being augmented where necessary and a national training plan is under development.

As HRSDC and SDC begin implementation of this management action plan we do so committed to coordinated efforts to build on our role as stewards of personal information and to maintain the trust that Canadians have placed in us.

1. INTRODUCTION

Background

This audit was initiated in Human Resources Development Canada (HRDC), which has since been reorganized into two new departments—Human Resources and Skills Development Canada (HRSDC), and Social Development Canada (SDC). The acronyms HRSDC or SDC are used in this report when the findings or recommendations apply to only one of the two new departments, and HRSDC/SDC is used when they apply to both. HRSDC/SDC is also used to designate the former department.

In the course of its operations, HRSDC/SDC collects and uses personal information from its clients and also receives personal information from other sources such as the Canada Revenue Agency (CRA—formerly the Canada Customs and Revenue Agency). In June 2001, CRA asked HRSDC/SDC to provide assurance that the personal information it transfers to HRSDC/SDC is handled in compliance with the *Privacy Act* and related policies.

In its annual Corporate Business Plan for 2003-2004, HRSDC/SDC has noted that Canadians are asked throughout their lives to entrust the Department with sensitive personal information and has committed to ensuring that the management of such information continues to meet, and is seen as meeting:

- All legislated privacy requirements and safeguards;
- The highest standards of respect for the privacy of personal information;
- The highest standards of security in the systems that collect and store this information.

HRSDC/SDC has recognized that these expectations must be met in order to sustain clients' willingness to share their information—particularly as the departments develop new channels of communication allowing citizens to conduct transactions electronically as well as through office visits, telephone calls, and mail.

Given the importance of properly managing personal information, HRSDC/SDC started to develop a formal Privacy Management Framework in 2000.

As part of the Departmental approach to retain the trust of Canadians in its handling of personal information, Internal Audit Services (IAS) was mandated in 2003 to conduct this audit to provide assurance that the access, use, retention, disclosure, and disposal of personal information:

- Were in compliance with the Privacy Act;
- Met Treasury Board and Departmental policies.

Scope of the Audit

This was the first time that an audit of the management of personal information has been conducted in HRSDC/SDC. Therefore, to determine the audit objectives and criteria the auditors went through extensive consultations with the Treasury Board Secretariat (TBS), CRA and the Office of Privacy Commissioner (OPC). Internal consultations were also held with HRSDC/SDC Privacy Directorate and with representatives of the programs and corporate services involved.

There is considerable complexity in the area of managing personal information. Personal information is physically and electronically spread among several systems, program areas, offices, and Regions. HRSDC/SDC has 320 in-person points of service in communities, 21 call centers and four Regional Information Technology Centers. Its core business touches millions of Canadians every day who rely on the departments to deliver programs and services. Therefore, personal information appears at least transiently on:

- Documents sent to those clients;
- Records of HRSDC/SDC clients;
- Computer storage in the form of tapes and disks;
- Computer screens accessed by employees across the country as they serve the clients.

Complexity is increased by the fact that many current policies, procedures and controls dealing with privacy are embedded within security policies. Security is a prerequisite to privacy, but the presence of security does not guarantee the coverage of privacy. For instance, the privacy principle that employees must only have access to the personal information needed to perform their function (need-to-know) is linked to the allocation and maintenance of User IDs. The allocation and maintenance of User IDs are primarily an information technology issue beyond the scope of this audit. Also, logical access to personal information often differentiates between a passive "read-only" capacity and an active "write and modify" mode, which is directly related to security but has little impact on privacy.

In April 2003, following consultations and risk assessments, the Audit and Evaluation Committee agreed that the audit would focus on four main program areas:

- Employment Insurance (EI);
- Old Age Security and the Canada Pension Plan (ISP);
- Financial Administrative Services–Departmental Accounts Receivable System (FAS-DARS);
- Strategic Policy (data used for policy analysis, research and evaluation activities).

The Committee also approved the following objectives[2]:

- Handling and protection of personal information is incorporated in the Departmental management framework;

[2] Initially, ten objectives were identified. Two of these, dealing with the collection of personal information, were left for a future audit. The remaining eight were regrouped into the six listed here for ease of reporting.

- Retention, protection and disposal of personal information meets Government Security Policies;
- Personal information is accessed only by authorized persons and used for the purpose for which it was collected;
- Personal information is disclosed in compliance with the *Privacy Act* and other applicable legislation, regulations, policies and agreements;
- Information on the nature and use of personal information is available to the public;
- Individuals have access to their own personal information and procedures are in place to handle complaints.

The detailed criteria for assessing whether or not the Department has met these objectives are listed in Appendix A. Fieldwork for the audit was conducted at National Headquarters (NHQ), in six Regions, six Regional Headquarters (RHQ), all four Information Technology Centres (ITC), and 34 offices and points of service (detail is presented in Appendix C) during the period from April to December 2003.

Methodology

The audit team collected evidence by:

- Reviewing documented policies, procedures and initiatives;
- Interviewing policy and operational staff and management at NHQ and RHQ;
- Interviewing management and operational staff in the offices visited;
- Analysing actual procedures and controls;
- Testing and observation.

Each Region visited was debriefed at the completion of the field visit. This national report is based on findings that were repeated across Regions and/or that had a national impact.

2. AUDIT FINDINGS

All significant audit findings are presented in this section in accordance with the audit objective(s) and criteria that are described in detail in Appendix A—Audit Objectives, Criteria and Methodology. Assurance statements on all of the criteria are included regardless of whether or not the performance expectations have been met.

In this report, "Privacy" is used as a generic term to designate the general management of personal information and the legislative and administrative framework that supports it.

Personal information is defined as information that is or can be related to an identifiable individual.

Confidentiality is the attribute of personal or non-personal information that should only be seen by persons with a right and a legitimate reason to do so. Confidentiality underpins the notions of "need to know" and "browsing" used in this report.

Audit Objective

The purpose of this audit is to provide assurance that the management of personal information within HRSDC/SDC is in compliance with the *Privacy Act*, particularly Sections 4 to 8 (commonly referred to as the *Code of Fair Information Practices*) and that the use, disclosure, retention and disposal of personal information conforms to Treasury Board Secretariat (TBS) and Departmental policies.

2.1 Objective 1: Handling and protection of personal information are incorporated in The Departmental Management Framework.

Audit Criteria

- Accountability for the protection and proper use of personal information is defined and documented;
- Policies, guidelines and procedures on the handling and protection of personal information are available and personnel have been informed and/or trained on these issues;
- Audit, monitoring, risk and control assessments on the handling and protection of personal information are performed on a regular basis.

2.1.1 Responsibility and Accountability

An increase in awareness by management and employees of their responsibilities in protecting the privacy and confidentiality of personal information was indicated during interviews.

HRSDC/SDC has displayed concerted effort to improve its handling of the personal information; several initiatives were launched to provide clearer policies, procedures and guidance on privacy.

1. The Privacy Management Framework Steering Committee (PMFSC) was established. It directs the development and implementation of the Privacy Management Framework, which defines responsibility and accountability on privacy from the Deputy Minister to employees and across programs. The PMFSC is also mandated to oversee the responses to corporate privacy policy issues.

2. The Databank Review Committee (DRC) is a senior-level committee that was established to review all of the department's policy analysis, research, and evaluation activities that require the linking of databanks and/or the use of unmasked (non-anomymized) personal identifiers.

3. The Information Technology Security Governance Committee (ITSGC) was established to provide direction, timely and effective oversight, advice, and guidance to the Information Technology Security function within HRSDC/SDC.

Several areas of the new departments—HRSDC and SDC—are interrelated. For instance, the delivery of EI services (and the handling of the corresponding personal information) is done through processing centres (HRSDC) and call centres (SDC). Some financial and administrative corporate services are common. This increases the need for an Accountability Framework that will address this reality and provide support and guidance to the two departments.

Recommendation No.1: (HRSDC/SDC)

Taking into account the interrelations and the sharing of personal information between the two departments, an Accountability Framework for the handling of personal information should be articulated, communicated and implemented at all levels as soon as possible.

Management's response:

The audit report has identified the importance of an accountability framework for the two departments to handle and protect personal information. In the last few years, HRSDC/SDC has been pro-active in developing and delivering a comprehensive Privacy Management Framework (PMF). This framework is comprised of four pillars: Strategic Planning and Governance, Risk Management, Cultural Change, and Assurance of Compliance. The implementation of the PMF supports both departments' commitment to the protection of personal information. As a result, the Privacy Management Framework Steering Committee has approved enterprise-wide accountabilities for Privacy and Security that include senior privacy officials for

HRSDC/SDC. The implementation of this instrument will formalize the privacy and security responsibilities from the Deputy Ministers to individual employees.

Other initiatives undertaken to increase the awareness of managers and staff include the development of an all encompassing Privacy Statement to enunciate the Departments' commitment for the proper handling of personal information, as well as education modules to complement corporate and operational training plans.

2.1.2 Policies, Guidelines and Procedures

Policies and procedures on privacy and security are available on the intranet and internet. E-mails and memos are used to inform employees of policies and procedures.

Current policies and procedures provide coverage of access by individuals to their own personal information held by HRSDC/SDC and disclosure of that information to themselves or their representatives. However, in the auditors' opinion, policies and procedures on the management of personal information generally focus on the security rather than the privacy aspect. For instance, access is often defined in terms of "read only" often referred to as "inquiry or view" or "write and modify" sometimes referred to as "update, adjudicate or approval" privileges that deal with the security rather than the confidentiality of the personal information. Similarly, interviews led the auditors to conclude that concerns for shipping material containing personal information by public carrier dealt more with its security than the protection of its confidentiality.

Recommendation No.2: (HRSDC/SDC)

Policies and procedures on the management of personal information should be reviewed to ensure that privacy is adequately and sufficiently covered.

Management's response:

The report identifies the need for a better implementation of the privacy and security components of the policies and procedures dealing with the handling of personal information. The current policies and procedures for handling personal information implicate Privacy, Information Management and Security experts in HRSDC/SDC: Privacy leads the activities of collection, use, retention, disclosure and disposal, Information Management is concerned with its retention, and Security focuses on the technical aspects of access, storage, transmission and destruction. This structure reflects Treasury Board Policies and Guidelines on Privacy and Data Protection, Management of Government Information Holdings, and Government Security, as well as, departmental policies, guidelines and procedures at the corporate and operational levels. In accordance with the Privacy Management Framework, and with the assistance of Privacy experts, HRSDC/SDC branches will review the adequacy and sufficiency of their policies and procedures for the handling of personal information.

Although, in the auditors' opinion, guidelines and procedures for teleworkers (employees who are allowed to bring documents home and work there) also deal mainly with security, privacy is generally adequately covered. The *Security Policy and Procedures Manual for the Human Resource Centres Canada* provides specific guidance for transporting and safeguarding of sensitive material at home, including a paragraph stating that "Precautions should be taken to ensure that sensitive files cannot be accessed by unauthorized persons, e.g. cleaners in a rented accommodation, or family or guests in the 'telework place.'" Teleworkers must sign an agreement to respect security and privacy rules. These agreements differ between Regions and some are more specific than others on the obligation to protect the confidentiality of the information and the rules that must be followed.

Members of EI Boards of Referees (an administrative tribunal composed of non-employees that hears appeals on Employment Insurance decisions) generally bring home appeal files containing personal information that may be sensitive. They sign an engagement to act with discretion by not discussing the content of the appeal files outside the boardroom and at the end of the day's session, members of the Board of Referees should return their copies of the appeal dockets to the Clerk of the Board for shredding in Confidential Waste, but not a formal agreement similar to the one applied to most teleworkers on the handling and protection of appeal files.

Recommendation No.3: (HRSDC/SDC)

Agreements signed by teleworkers should be standardized to ensure that the clauses dealing with the confidentiality of personal information are specific about the obligation to protect the confidentiality of the information and the rules that must be followed. Members of EI Board of Referees should be required to sign a similar agreement.

Management's Response:

While the report observed that privacy requirements were adequately covered for teleworkers, it also identified a need for a standardized approach. The Human Resources Branch, with the assistance of Privacy and Security experts, will review the use of standard clauses for teleworkers to ensure the consistent protection of personal information outside of departmental premises.

In regards to the Board of Referees, this body is independent and operates at arms-length from HRSDC and the Canada Employment Insurance Commission. HRSDC has no line authority over the Board of Referees or its individual members. Board of Referee members are subject to security screening and must sign an undertaking prior to their appointment. Once appointed, Board members are provided with the Board of Referees Policy and Administration (Subject 16 of the Insurance Services Policy Manual) which advises:

> *"Chairpersons and panel members should at all time be sensitive to the fact that the appeal dockets contain personal information. For this reason, at the end of the day's session, members of the Board of Referees should return their copies of the appeal dockets to the Clerk of the Board for shredding in Confidential Waste."*

Furthermore, over the last months the Insurance Branch has worked to further develop and implement policies and procedures to ensure that Board members are advised of their obligation to protect information originating from appeal dockets, hearings and decisions.

2.1.3 Information and Training

Awareness and understanding of expectations is an important aspect of the Privacy Management Framework. Interviews indicated that the understanding by managers and employees of their responsibilities to protect the confidentiality of personal information about clients and other individuals has increased.

Public Service Employment Act specifies that every new employee must sign an Oath of Office & Secrecy. Furthermore, employees who require access to personal information reported that they were given an overview of privacy-related issues during their initial training, with a focus on disclosure of personal information and conflicts of interest (e.g. handling the case of a friend or relative).

Formal training dealing specifically with privacy is available. An internet presentation has been developed to assist EI Privacy Coordinators to provide training and ISP is currently enhancing the privacy modules which will be available online at their college site in the summer of 2004. SP has also developed an Intranet presentation—Privacy Protocols for Research—for information sessions within their group.

Privacy training has been given to the Privacy Coordinators. At the time of the audit, specific privacy training was progressively reaching EI, ISP, SP and FAS (DARS) managers and employees. Employees and managers reported that privacy issues are now more frequently raised and discussed during staff meetings and information sessions.

At the time of the audit, communication and training plans on privacy existed but were not of a strategic nature and the level of coverage varied between Regions and Programs.

Recommendation No.4: (HRSDC/SDC)

A national strategic communication and training plan should be developed to ensure that all employees who have or may have access to personal information receive timely and adequate training and information on the legislation, policies and procedures for the use and protection of personal information in their area of activities.

Management's response:

The audit report recommends that a national communications and training plan be developed to compliment the operational training provided by branches and regions. Over the past three years, HRSDC/SDC has been developing a common understanding of organizational and employee values and ethics. The Human Resources Branch is leading the development of a National Training Plan to assess learning needs, and to design and adapt learning products to provide timely and adequate training on the use and protection of personal information. This plan will be implemented in partnership

with departmental branches and regions, and include contributions from the ATIP Directorates and FAS Security.

Until recently, Privacy Coordinators at the Regional and local levels dealt mainly with formal requests for disclosure of personal information and with access to information (ATIP) requests. One Regional Privacy Coordinator interviewed during the audit has adopted a proactive approach to the changing environment for privacy by developing training and reference material and initiating discussions on privacy issues. Others had more reactive attitudes and indicated they are waiting for guidance before making significant changes to the nature and extent of their activities.

To assess the degree of awareness and understanding by managers and employees of fundamental privacy principles during interviews, the auditors used the expression "need-to-know" to illustrate the principle that no employee should be given access personal information that is not required to perform his/her current functions. For example, giving employees access to screens containing personal financial information on clients would not meet the "need-to-know" principle if this type of information were not required by these employees to establish a benefit period or render a decision.

For the purpose of this audit, one particular type of violation of the "need-to-know" principle was called "browsing" and was defined as "looking at personal information about an individual without a legitimate business purpose." Browsing is not authorized in HRSDC/SDC and would be considered an offence, even if the browsing provided no personal advantage to the employee or implied no intended illegal use of the information. Most employees were aware that if such access were for unethical purpose such as personal profit, this would become a serious offence that could lead to severe sanctions.

During interviews, employees and managers mentioned that it was inappropriate to look at the file of a friend or relative. When prompted, they also mentioned that it was improper to look at any file or screen containing personal information if they had no valid business reason to do so.

As a result of the interviews with managers and employees, the auditors concluded that understanding and awareness of potential violations of the "need-to-know" principle could be strengthened.

Most managers and supervisors interviewed did not have precise knowledge of the nature and amount of personal information to which their employees are given access. When they request an access for a new employee or an employee who has new functions, they often copy the last request for an employee performing similar functions (this is generally referred to as "cloning"). More detail on the process of allocating access is given under Objective 3.

Recommendation No.5: (HRSDC/SDC)

Management should ensure that those who give and are given access to personal information understand the nature and application of the "need-to-know" principle and the consequences of violations such as "browsing" and unlawful disclosures.

Management's response:

We agree with the report's recommendation that the need-to-know principle and the consequences of its violation should be understood. In addition to the Human Resources Branch National Training Plan, regular awareness sessions will be conducted by FAS Security to ensure that the principle, and the consequences of its violation, are fully understood.

HRSDC/SDC is committed to protecting personal information. HRSDC/SDC will ensure that what it collects and creates is handled according to the Privacy Act and other applicable privacy protection laws. To verify that only those with a demonstrated need-to-know and who have been security screened to the appropriate level have access to personal information, the Policy and Guidelines for the Implementation and Monitoring of Audit Trails has been endorsed by the Privacy Management Framework Steering Committee.

As well, other initiatives are underway by EI, ISP and DARS to ensure that user access is related to a user profile. The review of user profiles is linked with the steps taken in support of Recommendation No. 10 that addresses the issue of attribution, maintenance and suppression of user IDs.

EI, ISP and DARS have undertaken the following initiatives:

- *EI user profiles are being developed to ensure that users access only the information they need to carry out their duties. A detailed statement of work and action plan is being undertaken by the Insurance Branch to analyse and review their policies and procedures;*
- *The ISP branch has reviewed and updated the access ISP system that is guided by user profiles. It will review and update its Operational Guidelines for requesting access, including the ISP User Access Request form and guide used by managers; and*
- *DARS will review the existing security grid to ensure that functions and duties and the associated security matrix properly align with the information available. This will involve a review of the screens associated with elements in the security matrix. Based on the outcomes of the review, defining revised business requirements will be undertaken to develop a revised security matrix, if required. Further, a review of existing policies and procedures will be conducted to identify gaps in support of this recommendation.*

2.1.4 Risk and Control Assessments

HRSDC/SDC and CRA have exchanged MOUs requiring each organization to periodically audit the management of the personal information received from the other. This is the first audit conducted in HRSDC/SDC under this agreement.

Risk and control assessments regarding on the handling and protection of personal information have been performed by EI and , ISP and SP at the National and Regional levels,. and in SP before the audit.

Since Treasury Board Secretariat introduced the new Privacy Impact Assessment (PIA) Policy in May 2002, new systems, programs and procedures must be reviewed and assessed for their impact on the collection, use and disposition of personal information. This policy will result in better awareness and coverage of the privacy risks associated with new or modified systems, programs and procedures.

2.2 Objective 2: Retention, protection and disposal of personal information meets Government Security Policies.

Audit Criteria

- Personal information is scheduled for retention and is disposed of in accordance with the Government Security Policy;
- Internal controls are in place to ensure that personal information is protected from unauthorized modification, erasure and destruction;
- Electronic databases containing personal information are protected from unauthorised viewing or copying and destruction, and tapes and other physical media containing personal information are protected and kept in secure places that are accessible only to authorized persons;
- Personal information is updated promptly when required and a record of the source of the information used to modify personal information is kept.

2.2.1 Retention and Disposition

Legal requirements or policies provide for retention of documents and other media containing personal information such as client files for at least six years.

In the offices visited, client files were kept on the premises for at least one year after the last administrative action. For the remaining prescribed period the files are sent to National Archives (NA) and then destroyed upon formal approval by the Department.

Dormant files were generally kept together with the active ones until they were ready to be shipped. Just before shipping to NA, they were packed in boxes. NA prescribes the sealing of boxes containing old client files when the office is situated outside of the NA city. When the office is in the same city as NA, the top flaps of boxes are only folded. The boxes, however, are wrapped together with a transparent plastic film. To have access to the file, the film must be removed (but it can be replaced afterward).

NA procedures require writing the first and the last file number on the front of each box. In the offices visited, the Social Insurance Number (SIN) is used as identifier. Three of the visited Regions wrote the full SIN of the first and the last file on the boxes, providing a valid and sometimes no longer used SIN to whoever sees or handles the boxes. One Region used only the last three digits. The practices in the other two Regions were not covered.

There are several methods used by HRSDC/SDC to dispose of personal information. Tapes and disks containing electronic personal information can be erased or physically destroyed. All the offices visited reported using safe destruction or safe erasing techniques. However, the tapes received from CRA or other Departments are returned in envelopes without being erased or destroyed.

Either HRSDC/SDC employees or a contractor using its own equipment shred paper containing personal information (computer print-outs, letters, sensitive waste, etc.) on the premises. Specialized companies are used to shred papers offsite.

HRSDC/SDC uses various carriers to ship material containing personal information to another location to be archived or destroyed. In the cities where they have a Branch, National Archives picks up the documents and takes charge and responsibility of the shipment when it is loaded on its truck. Where NA services are not available, HRSDC/SDC uses bonded carriers to ship documents, sensitive waste or other material. It is the practice in one location for an HRSDC/SDC employee to accompany the shipment, but this protocol was not reported elsewhere.

Auditors obtained and reviewed three copies of contracts for transportation and five for shredding documents or waste containing personal information. One of the three shipping contracts had a general clause on the protection of the confidentiality of the personal information while in transit or under the responsibility of the carrier:

> The Contractor shall treat as confidential, during as well as after the period of the contract, any information of a character confidential of the affairs of the Crown, to which their servant or agents become privy.

Three of the five shredding contracts had a very general clause on privacy.

With the above exceptions, the offices visited could not produce formal contracts for shipping or shredding of material containing personal information. Some offices were able to produce general hauling standing agreements or purchase orders with no privacy clause.

The Privacy Group has developed general clauses on privacy to be included in service contracts when personal information is involved but the examples provided to auditors did not cover contracts for shredding or transportation of personal information.

According to Legal Services, a shipping or shredding contract without a specific and binding clause on the protection of the confidentiality of the personal information would render the Department vulnerable in the case of litigation on wrongful use or disclosure.

Recommendation No.6: (HRSDC/SDC)

All situations where public companies are used to ship or destroy material that contains personal information should be covered by a contract that establishes and specifies the responsibility of the company to protect the confidentiality of the information while the information is under its control.

Only the last three digits of the Social Insurance Number should be indicated on boxes sent to National Archives.

Management's response:

The audit determined that there were some inconsistencies in service contracts for the shipping and destruction of material containing personal information and that standard clauses should be included in all shipping and shredding contracts. The HRSDC/SDC Access to Information and Privacy (ATIP) Directorates have been working with Legal Services to finalize these standard clauses. FAS Security will also undertake a review of the security aspects of these contracts. Discussions will occur between FAS Materiel Management and Public Works and Government Services Canada (PWGSC) to agree on the wording of clauses used in contracts awarded on behalf of HRSDC/SDC and to influence the development of their standard clauses for standing offers. In addition, a communications strategy and procedures are being developed to instruct procurement officers and privacy coordinators across both departments on the application of the appropriate clauses.

The report points out that the full SIN number should not be marked on the outside of boxes being shipped or stored outside of HRSDC/SDC facilities. Records management guidelines have been amended to advise that full SIN numbers should never be written on box exteriors and that they should only indicate the last three-digit-unit of the SIN being used to organize the files.

2.2.2 Access to Systems

As mentioned earlier, personal information about millions of clients exist in all Regions on paper files, documents, on tapes, and disks. Personal information also resides in several systems that are accessed through computers across the country.

HRSDC/SDC must protect the confidentiality and ensure legitimate use of this information, and as the custodian of the personal information the department must also protect it against unauthorized or inappropriate modification, erasure and destruction. When a legitimate modification is required, the Department must ensure it is done promptly and duly recorded. In computer systems the fundamental controls protecting the access to personal information are the passwords.

The logical access to ISP, EI, SP and FAS-DARS systems requires a password associated with a User ID. A password is a combination of letters and numbers that only its owner is intended to know. A User ID is also a combination of characters that

is generally assigned to an individual but it is not secret and more than one person can use it successively (unused User ID are sometimes recycled).

The password allocation process is primarily designed for security but it is covered here because security is a prerequisite to privacy.

When a User ID is allocated to an employee for the first time, this person is given a temporary password that can only be used once to access the password management screen. The employee chooses a personal secret password and enters it in the system. During the process, the employee is generally warned against sharing the password with anyone or leaving indications that would allow another person to discover or guess what it is. When these procedures and guidelines are followed, the employee is the only person who knows the secret password associated with his/her User ID and who can access the systems with this User ID.

Many HRSD/SDC employees must remember multiple passwords to access different systems in addition to the other passwords they use in other spheres of their life. Many of these passwords change periodically. Since a forgotten password causes inconveniences and delay, it is tempting to write it down on a piece of paper and hide it somewhere around the workplace. There is then a risk that another person will discover the password and wrongfully use it.

One of the Security Officers interviewed was aware of the risk and had found a way to increase password confidentiality. She asked employees to write down their passwords on a piece of paper and to put this paper in an sealed envelope. Then, she stored the envelope in her safe. If the password were forgotten, the employee would get the sealed envelope from the Security Officer, open it, retrieve the password and repeat the process. This is reported as an example of a simple and effective way to reduce the risk of password theft.

Password resetting/reactivation for mainframe computer systems may represent another source of risk. A password must be reset/reactivated when the employee has forgotten it (for instance, after an absence from work) or has entered it incorrectly several times in a row. The process to reset/reactivate a password starts with a call to one of the National Service Desks (NSDs). It was reported to auditors during their visits that in some cases the identity of the caller is not certified and no manager is involved in the process. If this happens, there is a risk that a person will obtain a new password that can be used to access personal information under an absent person's identity. IAS Information Technology (IT) team is currently pursuing this issue through their IT Security Audit to confirm the existence and nature of the risk. Specific observations and recommendations will be made at the completion of that exercise if appropriate.

2.2.3 Physical Protection of Files

The fundamental controls protecting paper files containing personal information are physical protection and premise access controls. Paper files containing personal information exist in EI (HRSDC), ISP and FAS-DARS (SDC).

In ISP (SDC) offices visited, client files were kept in locked rooms. In three Regions access was restricted to file management staff while elsewhere most employees had access. When documents are in use they are generally kept on desks and can be seen by those present on the floor.

In two FAS-DARS (SDC) offices visited, it was reported that active files were kept in a filing cabinet or room that was not locked at night.

In EI (HRSDC), files are generally kept on open shelves in the claim processing area, except in one office where files are kept in a room that must be locked at night. Employees taking out files are expected to record the withdrawal using a Docket Tracking System (DTS). However, this system is not designed to prevent the unauthorized withdrawal of a file, as there are no controls that ensure every file withdrawal is recorded.

In offices that provide in-person service, the rule is that the public is not allowed to enter the areas where the files are kept but there are exceptions. Clients may be called in for interviews or investigations, and service providers are given access to do repairs and maintenance. Local rules specify that these persons must be escorted while in the non-public area. Cleaning personnel generally have unescorted access to most office areas. The degree and consistency with which this access restriction is enforced could not be established during this audit, but during another audit, an audit team reported that they have entered restricted areas and remained there for several minutes before being approached.

The layout of the locations visited during the audit provided various degrees of protection against unauthorized access to material containing personal information. In some offices, a door with an electronic code-activated lock separated the public and restricted areas while in others there was only a barrier. In one Region, there was no physical separation between the public and the restricted area.

In three of the Regions visited where HRSDC/SDC uses facilities shared with partners, employees mentioned that preventing partners from seeing the personal information held by the Department was a difficult and sometimes delicate issue.

Recommendation No.7: (HRSDC/SDC)

Given the wide variety of situations calling for the protection of the confidentiality of client files, it is recommended that HRSDC and SDC conduct individual risk and control assessments in premises where documents containing personal information are stored to determine if the level of protection against unauthorized access or withdrawal of client files is adequate.

Management's response:

Security Officers conduct Threat and Risk Assessments (TRAs) of departmental premises that include consideration for the physical protection of client files. Furthermore, FAS Security will re-introduce the practice of conducting regular sweeps of NHQ facilities to assess compliance with the policies and procedures for safeguarding and transmitting

*protected and classified information. Regular security awareness training sessions are also given to employees***.**

2.2.4 Modification and Update

There are three reasons for modifying or updating the personal information of a client in EI (HRSDC), ISP and FAS-DARS (SDC):

- New data has been received under an agreement, such as a MOU with CRA;
- The agent collects new information during fact finding;
- A request is made by a client or a client's representative to update or modify a record.

In the first two situations, the modification is immediate and the client is not necessarily informed of the change unless this has an impact on his or her rights to benefits.

In the third situation, the request for change originating from the client or his/her representative can be received in person, by telephone or in writing. If in person, generally at a Human Resource Centre of Canada (HRCC), the employees reported that they verify the identity of the person with adequate questions and/or identification documents.

If the request is made by phone, generally received in a Telecentre, the employees reported that they ask the caller to provide personal information such as the SIN, date of birth, mother's maiden name or for EI, the Telephone Access Code (TAC). If the employee has doubts about the identity of the person, he/she may ask for additional information that only the client is expected to know such as benefit rate, date of claim, type of benefits, and whether the claim is active. If still in doubt, the Telecentre employee may refer the case to an Agent in a processing centre or an HRCC.

If the request is in writing, it is sent to a processing centre where the employees reported that they match the information on the request with the data in the systems or in the client's file, including the signature, if available.

When the person asking for the change is identified as a representative of the client, the employees must look for or obtain a written delegation or an authorization for disclosure signed by the client.

In most cases, once the identity of the client has been verified, the requested change is made immediately without challenge or further verification. This is especially true for changes of address, the most common request.

For ISP, policies for modification to personal information specify that evidence supporting the actions taken must be included in the file to justify changes made to client documents. For example, employees should keep on file a letter or notes from a telephone call from the client or his/her representative and any supporting documents. Five out of six ISP (SDC) offices and four out of five FAS-DARS (SDC) offices reported that they document the source of the change in the client files and keep on file a copy of any relevant document.

For EI (HRSDC), auditors were unable to find policies or procedures concerning the documentation of changes in a client file and reported recording practices varied. In some Regions, agents are instructed to document the source of the change and file or keep a copy of evidence documents presented by the client. In others, this is left to the employee's judgement and discretion with an emphasis on the paperless approach.

A lack of documentation supporting a change made to a client's file can, in some circumstances, present a risk. The change may have been unjustified or inaccurate; the request for change could have been received from someone other than the client or an authorized representative, or as with all changes a factual error may have been made. Should this occur and cause hardship or affect the integrity of the program, it would be difficult to trace back the change without supporting documentation.

All employees reported that a request for a change of personal information is almost always processed immediately. At the Telecentre, most changes are made while talking with the client. Requests for changes that they are not capable or authorized to do at the Telecentre are sent to an HRCC by electronic mail. At offices, the delay to process a change may vary but they are normally done within 48 hours.

Recommendation No.8: (HRSDC)

The rules and procedures for recording the source and the reason for changes to personal information and for keeping evidence documents should be clarified to reduce the risks of inappropriate changes that may cause hardship.

Management's response:

While the audit report points out that requests for changes to personal information made to client files are done in a timely manner, it also observed that the procedures for these changes vary between programs. In the case of EI, a national directive will be issued to clarify the policies and procedures for documenting the source and reason for change. ISP will continue to ensure that its policies and procedures for the modification of personal information remain compliant with the audit observation.

2.3 Objective 3: Personal information is accessed only by authorized persons and used for the purpose for which it was collected.

Audit Criteria

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

- Requests to provide or modify access to personal information originate from an authorized person;
- The level of access requested matches the current position and functions of the person for whom this access is requested;
- The access profile of an employee whose status, position or function has changed is modified, suspended or removed if required;

- Use of personal information is directly related to an operating program or activity and is consistent with the original purpose for which the information was obtained or compiled;
- Viewing of personal information is monitored regularly to detect unauthorized or unjustified access through audit trails or other appropriate means of control;
- Personal information used for policy analysis, research and evaluation is anonymized before use or disclosure unless otherwise authorized;
- Personal information used for administrative purposes or program management that is not anonymized is protected from unauthorized access or use;
- Data matching and record linkages are consistent with the stated purpose for which the information was obtained or compiled;
- Data matches for administrative purposes and record linkages for non-administrative research purposes that use personal information meet the requirements of applicable policies—the Treasury Board Policy on Data Matching and HRSDC/SDC policies on record linkage;
- Material containing personal information is identified as "Protected" and handled in accordance with the Privacy Legislation, the Government Security Policy and other applicable legislation, regulations and policies;
- Procedures exist to handle security violations or disclosure of personal information in error.

2.3.1 Attribution, Maintenance and Suppression of User IDs

HRSDC/SDC holds personal information on its clients and other persons on paper files, tapes and disks, but most of it is held in the various systems supporting ISP, EI and FAS-DARS programs and operations. The protection of paper files was discussed in section 3.2.3 of this report. This section focuses on access and use of personal information stored in the systems.

Passwords and User IDs were defined and the need to protect the confidentiality of passwords was discussed in section 3.2.2 of this report, and the "need to know" principle was discussed in section 3.1.3. Another key concept in the control of access to personal information is the profile associated with a User ID. A profile is a set of codes attached to a User ID that enable accesses to the specific programs and screens required to perform a function such as the calculation or creation of an EI benefit period. In the auditors' opinion, when it establishes segregation of duties and limits access to certain functions User ID profiling is primarily a security control, but it is also a privacy control as it determines what personal information can be accessed.

The "need to know" principle requires that the profile provide access to only the personal information an employee requires to perform his/her present legitimate function. Therefore, the profile must initially be correctly determined and then adjusted when a change in the status or function of that employee affects these requirements.

From a privacy point of view, proper profiling implies that the screens containing personal information have been identified for each system and program and that the screens an employee needs to access to perform his/her functions have been determined. The legitimate access to a specific client file was discussed in section 3.1.3.

The following is an overview of the process for the profiling, allocation and maintenance of User ID. The complete details of such a complex process is beyond the scope of this audit, and only the aspects that are directly related to privacy are covered.

For EI (HRSDC) and FAS-DARS (SDC), at least three persons must be involved in a User ID request: the employee, a supervisor or manager and an Information Technology (IT) Security Officer in one of the four Information Technology Centres (ITCs). The designated person/Local Security Officer in an office is the only person authorized to send the request to the ITC. A designated person/Local Security Officer could be the employee's manager or supervisor, administrative staff or a Micro Support Specialist (MSS).

For ISP (SDC), in addition to the three parties identified for the EI process the request goes through a Security Administrative Control Officer (SACO) who is the only person authorized to send the request to the ITC.

ISP, EI and FAS-DARS' managers, designated persons/Local Security Officers and SACOs reported to visiting auditors that they follow the process and use the e-forms when requesting the ITC to modify or cancel an access privilege with the exception of one ITC which reported accepting requests under other forms.

For SP, the employee, his/her manager/supervisor, a Data Development Top Secret Systems (TSS) Security Officer and a Departmental Security Officer from Systems in NHQ are involved. Where the program area wishes to access personal information maintained by Data Development, the Data Development TSS Security Officer is the SP authorized person who is the intermediary between programs and systems. SP uses the Government Telecommunications and Informatics Services (GTIS) mainframe to store data and access to this mainframe requires the ADM's approval.

Representatives from EI, ISP and FAS-DARS were interviewed to assess to what degree each one knew his/her level of responsibility and the responsibility of the other persons involved in the process. The majority of supervisors and managers understood that they were ultimately responsible for the access given to their employees. They said they had general reference documentation on access to systems for various positions but that it did not indicate the proper access to be given to employees to meet privacy requirements. As mentioned in section 3.1.3, few managers and supervisors have a precise knowledge of the nature and amount of personal information their employees are given access to. Most relied on the designated person or the IT Security Officer at the ITC to determine and provide the right access. In the offices visited, new access requests were generally copies of the access previously given to employees doing a similar job (this was called "cloning")

At the ITC, the IT Security Officers knew the profiles usually associated with a function but did not know the specific type of information—personal or not—that the profiles enable a user to access. If the requested profile seemed unusual, the IT Security officer may contact the requestor for verification. Ultimately, though, they provided the profile requested and relied on the requestor to comply with the applicable procedures.

Recommendation No.9: (HRSDC/SDC)

For all the persons involved in the process of management of all User IDs and profiles providing access to personal information, responsibility and accountability should be clearly defined and implemented.

Documentation should be available on the nature of the personal information the employee is given access to.

Management's response:

With this recommendation the audit report identifies the application of user profiles in the attribution of user IDs. In conjunction with management's response to Recommendation No. 5, the branches for EI, ISP and DARS have undertaken the following actions:

- *In addition to the work to strengthen user profiles that will ensure that users are only granted access to the information that they need to carry out their duties, the Insurance Branch is working with the Systems Branch to analyse and review procedures and policies that will reinforce the process for creating, modifying, and deleting user IDs;*
- *ISP will complete a comprehensive review of all user profiles; and*
- *DARS will post a document on the Intranet clearly defining the roles of those involved in establishing a DARS user ID.*

Managers and employees interviewed from EI, ISP and FAS-DARS were of the opinion that access held by employees reflected their position and/or status and that all accesses were modified or cancelled when required. Limited testing conducted during the audit indicated that the status of employees is not always updated. A comprehensive test is planned to determine the extent of the problem (see Test in Section 3.3.2 below).

EI (HRSDC), ISP and FAS-DARS (SDC) have initiated a comprehensive review of all access profiles to ensure the proper access to personal information for all groups and functions, in respect to the "need-to-know" principle. This exercise was not completed in any of these groups at the time of writing this report.

For SP, accesses are granted for a pre-determined limited period of time.

Recommendation No.10: (HRSDC/SDC)

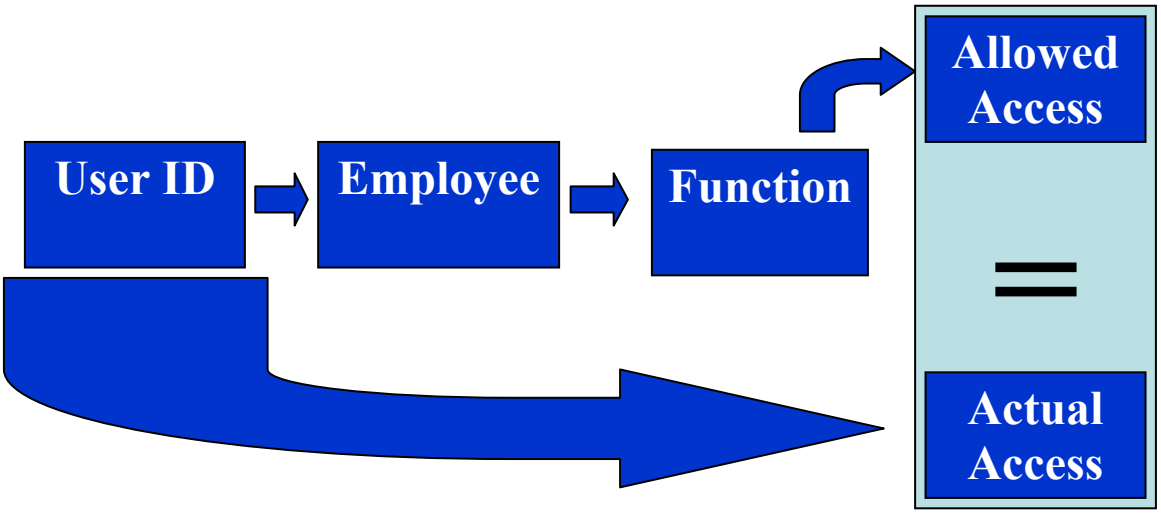
Accountability and responsibility for the attribution of User IDs that meet the privacy requirements should be defined, understood and accepted.

Management's response:

The audit indicated that a comprehensive review of user profiles would ensure that the issuance and maintenance of user IDs is appropriate. To this effect, the Systems Branch, with the participation of FAS Security and the Human Resources Branch, is reviewing the existing documentation and procedures on all aspects of the issuance and maintenance of user IDs to ensure compliance with the Privacy Act, Treasury Board and Departmental policies, and industry best practices. This will support other recommendations made in the audit report to strengthen the access to systems based on the need-to-know principle and in relation to user profiles. Responsibilities for user profiles and user IDs have also been included in the enterprise-wide accountabilities for Privacy and Security that were approved by the Privacy Management Framework Steering Committee.

2.3.2 Test

The audit team initially planned a test to provide assurance that the level of access to EI, ISP and FAS-DARS systems matched the "need to know" privacy principle. SP was not included in this test because they do not have access to the mainframe and their activities are different from the other programs selected. The concept and methodology of this planned test are illustrated and described below:



1. A random, representative sample is drawn from all the active User IDs that provide access to EI, ISP and FAS-DARS programs containing personal information.
2. The proper (legitimate) incumbent of the User ID is identified.
3. The function exercised by the incumbent is determined for a given period.
4. The actual access (provided by the profile of the User ID) is compared to the privacy compliant access allowed for that position and for that period.
5. A match indicates that the "need to know" principle is respected.

Several difficulties were encountered in the early stage of the test. These were:

- Defining and obtaining a certified list of all the active User IDs providing access to EI, ISP or FAS-DARS programs and databases containing personal information;
- Identifying with certainty the incumbents of a User ID when there were two or more homonyms (HRSDC/SDC's unique employee identifier, the PRI, is generally not used for User IDs);
- Identifying the function exercised by some of the incumbents during the period of reference. The terminology used to describe functions is not consistent and the auditors ended up with more than one hundred job titles while there are many fewer distinct functions in the area covered;
- Obtaining grids clearly linking a function to an access that met the need-to-know principle.

After a few weeks, it became clear that completing the test would have required excessive use of resources and even if it had been completed the accuracy of the results would not have been assured. It was decided to postpone the test until conditions allow IAS to conduct the test in an efficient and effective way that will provide results with the required level of integrity and accuracy. The fulfilment of these conditions will also allow EI, ISP and FAS-DARS to conduct their own monitoring of accesses thereafter.

Recommendation No.11: (HRSDC/SDC)

To allow management to effectively and efficiently monitor access to personal information, and to facilitate periodic audits, the following should be created as soon as possible:

1. *A list of all the User IDs that provide access to EI, ISP or FAS (DARS) programs and databases containing personal information, certified by the proper level of authority (to be identified in the Privacy Accountability Framework presently under development);*
2. *Practical processes to determine with certainty the identity of the incumbent of each of the User ID listed in (1)*
3. *Practical processes to determine with certainty the function exercised by each incumbent identified in (2)*
4. *Grids linking each function identified in (3) to an access profile that meets privacy requirements.*

Management's response:

Management agrees with the recommendation to monitor access to personal information and has taken action. The Systems Branch will produce a list, for the verification of RC managers, of all user IDs, including those that provide access to EI or DARS, and will establish, in cooperation with FAS Security, practical processes to determine the identities of all those assigned user IDs. For verification purposes, the Systems Branch will identify to managers the access capabilities of their users. Branches are responsible to approve and restrict the information that can be viewed or modified within their area. As indicated in management's response related to the review of user profiles in

recommendation No. 9, the branches for EI, ISP and DARS will review their user profiles and will identify each user's profile. The Systems Branch will then match that information to the appropriate user ID within Security Management and Single Logon.

With respect to DARS, a list of all users accessing the database has already been established, and a user ID may only be issued when a PRI has been associated to it. In addition, the function exercised by each DARS user is identified in the user profile and a security matrix has been developed to link functions and duties with access privileges.

2.3.3 Use and Viewing

All the managers and employees interviewed agreed that access to personal information must be restricted and used only for the purpose of delivering HRSDC/SDC programs and services.

Policies and procedures to deal with conflicts of interest are in place. Managers and employees mentioned the need to avoid potential conflict of interest situations. Files of family members or friends must be processed by other employees, in another office if necessary, and must be kept in locked cabinets with limited access for employees.

Employees also mentioned the duty of not disclosing personal information to unauthorized persons. Specific policies and procedures on the disclosure of personal information exist and are addressed later in this report.

The "need to know" privacy principle and the violation of the "need to know" principle referred to as "browsing" were defined in section 3.1.3. To prevent and detect browsing, the most effective control in the opinion of the auditors is the monitoring of accesses to personal information through an audit trail such as the one described in the next section.

2.3.4 Protected

PROTECTED

PROTECTED

Recommendation No 12: (HRSDC/SDC)

PROTECTED

Management's response:

PROTECTED

2.3.5 Anonymization of Personal Information

To ensure that access is limited by the need-to-know principle, SP—the major user of data for policy analysis, research and evaluation activities—has developed a protocol for handling and using databases containing personal information.

In SP, only six individuals of Data Development (five Programmers and one Administrative Assistant) can access files and view personal information before anonymizing (masking) of the data. Each has access to their assigned project.

When SP receives files from other departments such as CRA, the programmer enters the data into the systems and anonymizes it using masking, encryption or replacement. Each databank is masked in a different way in order to prevent files being linked with the identity of a person. Data in this form can be used for surveys, research or analysis. Access is requested on an individual basis for each employee and for each project. The source files are returned to the originators and non-anonymized information does not remain within Data Development.

2.3.6 Data Matching and Record Linkages

All identified data matching and record linkages are done at the National Headquarters, These matches, essentially done for Investigation and Control (I&C) and SP activities, must be explicitly authorized and covered by a specific agreement.

As per TBS policy, the Office of the Privacy Commissioner (OPC) is consulted when new matches in EI and ISP are requested and the only person empowered to approve a data match is the Director of the Access to Information and Privacy Directorate. In most cases the match is between fiscal data received from CRA and program data collected by HRSDC/SDC. In general, data matching activities are recurrent and automated. Most data matches are performed on a routine basis, mainly for investigation and control purposes.

In SP, record linkages for research purposes are not routine. Each occurrence must be reviewed by the DRC and OPC and approved by the Deputy Minister (DM).

2.3.7 Labelling of Personal Information

An Information Classification Guide issued by the Security, Investigations and Emergency Response Branch was sent to all HRSDC/SDC employees in 2002.This guide provides definitions and instructions on the level of protection and the safeguards and procedures to be followed for different types of documents containing personal information.

We found that the interpretation of the Guide varied. For instance, the Guide provides broad definitions of the levels of protection "A" and "B" but in many cases it is a matter of judgement. We also found that the Guide was not consistently applied. For instance, it was reported that some offices use a non-secure fax to send client information. In other cases, they send client information by fax but they could not confirm that the fax was secure. This practice would not protect the confidentiality of the information if the documents were sent to the wrong place. It was reported that protected information is being sent from HRCCs to clients and insurability rulings to CRA in a single envelope.

The files of clients are regularly moved between processing centres. It was reported that the files were shipped in double envelopes.

During a preliminary assessment the auditors were told that the double envelope for protected documents was regarded as a "best practice" but not a mandatory procedure.

SP has developed directives on the protection of personal information used for policy analysis, research and evaluation activities within their group. This has been communicated to staff and discussed in information sessions. In SP, CDs are labelled "protected B" and information sent outside of HRSDC/SDC is labelled "protected" at the appropriate level.

Recommendation No.13: (HRSDC/SDC):

The Information Classification Guide should be supplemented with guidelines that provide practical guidance on the classification and handling of the documents containing personal information that are most frequently used by the various programs.

Internal controls should be put in place to ensure that protected material is identified and handled according to its level.

Management's response:

The audit report noted that the Information Classification Guide issued by Security may not always be well understood. FAS Security at NHQ has undertaken the development of guidelines to clearly explain the full spectrum of handling, safeguarding, transmitting and destroying personal information and other sensitive information. Security will re-introduce the practice of conducting regular sweeps of NHQ facilities to assess compliance with the policies and procedures for safeguarding and transmitting protected and classified information. Regular security awareness training sessions are also given to employees.

2.3.8 Handling of Violations

Regional and local managers indicated they would report any instances of security violations or disclosure of personal information in error to Security or to the Human Resources Branch, depending on the circumstances. In NHQ, managers mentioned that the process to be followed in these cases was not clear to them.

Recommendation No.14: (HRSDC/SDC)

The process to be followed by managers and employees who become aware of a possible privacy violation should be clarified and communicated.

Management's response:

The recently revised Departmental Guidelines for Conducting Administrative Investigation clarifies the policy and procedures to be followed by employees and managers when reporting suspected incidents of privacy violations or other issues of administrative or criminal wrongdoings. These guidelines were sent to Regional Offices and are available on the Intranet.

2.4 Objective 4: personal information is disclosed in compliance with the *Privacy Act* and other applicable legislation, regulations, policies and agreements.

Audit Criteria

- The authority to disclose personal information is clearly established and documented, the disclosure process meets the applicable policies and procedures and the nature and amount of personal information disclosed is limited to the purpose of the disclosure.

2.4.1 Disclosure of Personal Information[3]

The authority to disclose or not to disclose personal information to clients is contained in the legislation and regulations of HRSDC/SDC programs and in MOUs when the information is received from a third party.

Requests for access to personal information are classified as formal or informal. A formal request is either a request received in writing that refers to the *Privacy Act* or a request presented on the official Info Source form. Formal requests must be responded to in writing within 30 days. The response must inform about the client's right to ask for correction of the information held by HRSDC/SDC and the right to complain.

The Privacy Coordinator at the local level processes formal requests for disclosure. The Department has the right not to disclose specific personal information under certain circumstances; this is called an exemption. Examples of exemption are personal information received from law enforcement and investigations, information about another individual, medical records and information that would jeopardize the safety of individuals. For EI (HRSDC), NHQ stated that every Regional Privacy Coordinator is allowed to handle exemptions, but mentioned that some of them do not want to handle these exemptions. Two Regional Coordinators interviewed told the auditors that they do not have authority to process exemptions. For ISP (SDC), all exemptions must be handled at NHQ unless the Local or Regional Privacy Coordinator has been delegated this authority.

The review showed that local offices and Regional Privacy Coordinators followed the procedures when responding to formal requests for disclosure. The amount of information disclosed was limited to the information requested. In five Regions out of six, the letter sent mentioned the client's rights for requesting correction and complaint.

An informal request is one received verbally or in writing but with no reference to the *Privacy Act*, or one that is not presented on the official Info Source form. It is to be noted that the nature of the information to be disclosed is not a consideration, although the sensitivity of the information disclosed may be the same or higher than that of a formal request. At the local level any agent handles informal requests, or sometimes by the Privacy Coordinator.

[3] This section deals with the disclosure of personal information by HRDSC/SDC to individuals. Disclosure of personal information to other organizations, departments or level of government will be handled in future audits.

Verbal informal requests for disclosure are not documented. Interviews showed that the procedures for documenting written informal requests vary between programs and offices. Inappropriate disclosure of personal information could have the same negative consequences as the inappropriate change of personal information discussed earlier and for the same reason it should be documented in certain situations.

Employees who were interviewed understood their responsibility not to disclose personal information to unauthorized persons. The same identification process is used as that described under 3.2.4 when a client or a representative requests a change. The disclosure is made once the identity of the client has been verified, unless the information meets an exemption criterion.

In EI (HRSDC), the Local Privacy Coordinator keeps a log of all formal requests and sends it to the Regional Privacy Coordinator once a month. The Regional Privacy Coordinator compiles the results received from local offices yearly and sends the statistics to NHQ. In ISP (SDC), the Local Privacy Coordinator compiles the requests once a month and sends them to NHQ, which compiles the statistics received from Regions once a year. Statistics for formal and informal requests are sent to the Program Assistant Deputy Minister (ADM) and only the statistics for formal requests are sent to the Parliament.

Recommendation No.15: (HRSDC/SDC)

The nature and sensitivity of the information disclosed should be taken into account in the distinction between formal and informal disclosure and the rules for documenting the disclosure should be reviewed.

The rules and procedures for recording the source and the reason for informal disclosure of personal information should be clarified.

Management's response:

Training materials and existing branch policies and guidelines will be examined to ensure that they address the documentation of informal requests, including verbal inquires, that involve the disclosure of personal information.

2.5 Objective 5: Information on the nature and use of personal information is available to the public.

Audit Criteria

- All HRDC personal information holdings are accurately described in Treasury Board Secretariat Info Source publications;
- Any new programs or services, or significant changes to existing programs or services, that involve the collection, use or disclosure of personal information and affect privacy, are in compliance with Treasury Board's Privacy Impact Assessment Policy;
- Summaries of Privacy Impact Assessments (PIAs) are made available to the public;

- Where appropriate, a communication strategy exists to deal with public concerns and perceptions about privacy.

2.5.1 Info Source

Information on the nature and use of personal information is available to the public through Info Source, which describes the organization of the Government of Canada and its information holdings. The information holdings include Program records and Personal Information Banks.

The report about each personal information bank includes a description of the personal information and statements about the uses and disclosures of it. There is a standard government process to update these reports. Every year, the Privacy Group is responsible to initiate a process by which all Programs review their area of responsibility. The Privacy Group compiles and sends a consolidated report to TBS. Info Source is also updated if required following a PIA.

2.5.2 Privacy Impact Assessment

The responsibility to identify the need for a PIA is shared between various levels in HRSDC/SDC. Executive management in NHQ and in the Regions are responsible for the identification of programs and activities that require a PIA submission while program and service managers are responsible for its preparation. Departmental Privacy Coordinators assist in the development of PIA submissions. The Deputy Minister is responsible for the approval of the PIA, following a positive recommendation from the PMFSC. PIA submissions that are recommended for approval also undergo review by the Office of the Privacy Commissioner (OPC).

TBS policy requires the publication of a PIA summary. HRSDC/SDC is only at the beginning of the process and there have been no PIA summaries published to date.

2.5.3 Public Concerns

Potential breaches of privacy are reported in accordance with Departmental security procedures and are investigated by the Security, Investigations and Emergency Response Directorate. The Access to Information and Privacy Directorate is informed of the potential breach and determines whether or not the OPC should be informed, based on the sensitivity of the case at hand. The OPC then determines the level of their involvement.

The program area where the potential breach occurred must work with Communications to prepare media lines.

2.6 Objective 6: Individuals have access to their own personal information and procedures are in place to handle complaints.

Audit Criteria

- Individuals are informed of their rights to have access to their personal information;
- There is a process by which an individual may access and discuss or challenge the accuracy of his/her record;
- There is a process by which an individual is notified that a change has been made to his/her information;
- Individuals are provided with access to their personal information in the official language of their choice and in alternative format;
- Complaint procedures are consistent with legislated requirements.

2.6.1 Access to Personal Information

According to the managers and employees interviewed, HRSDC/SDC clients are informed of their right to access the content of their file through the Web site, application forms and also verbally when appropriate.

As mentioned, in five Regions the letters sent to clients in response to a formal request indicate their right to review and challenge the content of their files. In Telecentres, this is done informally and verbally.

As indicated previously, clients are not automatically informed of changes to their file unless it has a direct and immediate impact on their right to benefits.

All offices visited are committed to providing clients with access to their personal information in the official language of their choice and in the format required, but they mentioned that in some circumstances this could delay the processing of the request.

2.6.2 Complaint Procedures

All Regions reported that a mechanism is in place to handle privacy related complaints. Complaints are generally processed by the OPC. Some Regions reported taking proactive measures to try to rectify the situation before sending the case to the OPC.

The outcome of complaints are not automatically shared with the Regions unless it leads to a recommendation from the OPC to change procedures, in which case auditors were told that this would be communicated to all Regions.

3. CONCLUSION

The auditors conclude that:

- HRSDC/SDC is displaying concerted effort to improve its handling of the personal information it holds about its clients and other persons and several initiatives have been launched to improve the protection of personal information and ensure the information is accessed and used for legitimate purposes;
- Policies and procedures covering all aspects of the management of personal information are in place, either as stand alones or mixed with security. Three senior-level committees devoted to privacy have been created. Accountability is being redefined or clarified through the development of a Privacy Management Framework.;
- A national strategic communication and training plan is recommended to ensure all employees receive timely and adequate training and information on the legislation, policies and procedures for the use and protection of personal information in their area of activities;
- The work initiated on audit trails, profiling and management of User IDs should be completed to ensure the proper access to personal information for all groups and functions.

Overall Opinion

Based on our audit work, it is our opinion that important progress has been and is continuing to be made in the management of personal information.

Nevertheless, further improvements are required per our recommendations.

Management has developed an appropriate action plan (Appendix B) to address these recommendations. Its successful completion, especially regarding recommendations 9 to 12, should put in place all the expected controls for the appropriate management of personal information within HRSDC and SDC.

In our professional judgment, appropriate audit procedures have been followed and sufficient evidence has been gathered to support the conclusions contained in this report. The conclusions are based on the situation that existed at the time of the audit against the audit criteria. The conclusions apply only to the management of personal information activities examined.

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.

Overall Management's response

The Director General, Privacy, together with the Privacy Coordinators for HRSDC and SDC, and Directors General from several branches, have reviewed the Audit of Management of Personal Information and collaborated on the preparation of its accompanying management action plan.

The concern that Canadians express for their privacy continues to increase, and the broad availability of integrated service offerings, often through new electronic channels, is one contributing factor. Canadians want assurance that their personal information is being carefully managed within well-defined parameters. The Privacy Act and related program authorities set out our obligations to protect personal information and to ensure its appropriate collection, use and disclosure. These legislative authorities are complemented with policies, procedures and tools that have been the subject of this review.

The internal audit and management action plan represent a key step in the ongoing implementation of the award-winning Privacy Management Framework (PMF). The PMF, and its four pillars of Strategic Planning and Governance, Risk Management, Cultural Change, and Assurance of Compliance, are focusing departmental attention onto privacy matters. Considerable progress has been made and the Departments have been recognized for their initiative.

Together, the PMF and this audit serve to demonstrate how we uphold our obligation to protect the personal information of Canadians. For the past two years HRDC has recognized Privacy as a strategic corporate priority under the goal of Service Excellence. This is explicit recognition, at the highest departmental level, of the importance of privacy to Canadians and their expectations of government to protect it. Both HRSDC and SDC are expected to continue this commitment to the effective management of personal information and incorporate it as an intrinsic component of their respective cultures. As the audit has clearly demonstrated, the effective management of personal information is no different than that of any other strategic asset. This is why controls are being augmented where necessary and a national training plan is under development.

As HRSDC and SDC begin implementation of this management action plan we do so committed to coordinated efforts to build on our role as stewards of personal information and to maintain the trust that Canadians have placed in us.

APPENDIX A: AUDIT OBJECTIVES, CRITERIA AND METHODOLOGY

Initially, ten objectives were identified for this audit. Two of these, dealing with the collection of personal information were left for a future audit. The remaining eight have been regrouped into six for ease of reporting. The original ten objectives can be found in the Terms of Reference issued in March 2003.

Objective 1:

Handling and protection of personal information are incorporated in the Departmental management framework. (Objective 1 of TOR)

The following criteria were used to examine personal information practices to ensure that:

1.1 Accountability for the protection and proper use of personal information is defined and documented;

1.2 Policies, guidelines and procedures on the handling and protection of personal information are available;

1.3 Personnel have been informed and/or trained on these issues;

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

Objective 2:

Retention, protection and disposal of personal information meets Government Security Policies. (Objectives 4 & 5 of TOR)

The following criteria were used to examine personal information practices to ensure that:

2.1 Personal information is scheduled for retention and is disposed of in accordance with the Government Security policy;

2.2 Internal controls are in place to ensure that personal information is protected from unauthorized modification, erasure and destruction;

2.3 Electronic databases containing personal information are protected from unauthorised viewing or copying and destruction, and tapes and other physical media containing personal information are protected and kept in secure places that are accessible only to authorized persons;

2.4 Personal information is updated promptly when required and a record of the source of the information used to modify personal information is kept.

Objective 3:

Personal information is accessed only by authorized persons and used for the purpose for which it was collected. (Objectives 6 & 7 of TOR)

The following criteria were used to examine personal information practices to ensure that:

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

- Requests to provide or modify access to personal information originate from an authorized person.
- Level of access requested matches the current position and functions of the person for whom this access is requested.
- The access profile of an employee whose status, position or function has changed is modified, suspended or removed if required.

3.2 Use of personal information is directly related to an operating program or activity and is consistent with the original purpose for which the information was obtained or compiled.

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

3.4 Personal information used for policy analysis, research and evaluation is anonymized before use or disclosure unless otherwise specified.

3.5 Personal information used for administrative purposes or program management that is not anonymized is protected from unauthorized access or use.

3.6 Data matching and record linkages are consistent with the stated purpose for which the information was obtained or compiled.

3.7 Data matches for administrative purposes and record linkages for non-administrative for research purposes that use personal information meet the requirements of applicable policies—the Treasury Board Policy on Data Matching and HRSDC/SDC policies on record linkage.

3.8 Material containing personal information is identified as "Protected" and handled in accordance with the Privacy Legislation, the Government Security Policy and other applicable legislation, regulations and policies.

3.9 Procedures exist to handle security violations or disclosure of personal information in error.

Objective 4:

Personal information is disclosed in compliance with the *Privacy Act* and other applicable legislation, regulations, policies and agreements. (Objective 8 of TOR)

The following criteria were used to examine personal information practices to ensure that:

4.1 The authority to disclose personal information is clearly established and documented, the disclosure process meets the applicable policies and procedures and the nature and amount of personal information disclosed is limited to the purpose of the disclosure.

Objective 5:

Information on the nature and use of personal information is available to the public. (Objective 9 of TOR)

The following criteria were used to examine personal information practices to ensure that:

5.1 All HRSDC/SDC personal information holdings are accurately described in Treasury Board Secretariat Info Source publications.

5.2 Any new programs or services, or significant changes to existing programs or services, that involve the collection, use or disclosure of personal information and affect privacy, are in compliance with Treasury Board's Privacy Impact Assessment Policy.

5.3 Summaries of Privacy Impact Assessments (PIAs) are made available to the public.

5.4 Where appropriate, a communication strategy exists to deal with public concerns and perceptions about privacy.

Objective 6:

Individuals have access to their own personal information and procedures are in place to handle complaints. (Objective 10 of TOR)

The following criteria were used to examine personal information practices to ensure that:

6.1 Individuals are informed of their rights to have access to their personal information.

6.2 There is a process by which an individual may access and discuss or challenge the accuracy of his/her record.

6.3 There is a process by which an individual is notified that a change has been made to his/her information.

6.4 Individuals are provided with access to their personal information in the official language of their choice and in alternative format.

6.5 Complaint procedures are consistent with legislated requirements.

SCOPE

The audit examined the use, communication with others and security of personal information in Employment Insurance, Income Security Programs, the Departmental Accounts Receivable Services (DARS) and Strategic Policy.

The audit focused on personal information received from Canada Customs and Revenue Agency (CCRA) but covered wider Departmental controls and systems where it is not possible or practical to identify or segregate the part of the control or system that is directly related to the personal information received from CCRA. This includes, but is not restricted, to the generation and attribution of User ID giving access to personal information, the protection of associated passwords, the physical and logical protection of documents and electronic databases.

This project covered the National Headquarters, the four Information Technology Centres and selected Regional Headquarters and points of service across the country.

METHODOLOGY

The audit team identified and assessed appropriateness of internal controls related to the protection of personal information and determined whether the objectives and standards applicable to the management of personal information listed in this document, are met.

This audit assignment used standard audit tools and methodology including individual and group interviews, on-site observations, document review and analysis, statistical analysis, flowcharting and analytical audit procedures.

APPENDIX B: MANAGEMENT ACTION PLAN

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
1) An Accountability Framework for the handling of personal information should be articulated, taking into account the interrelations and the sharing of personal information between the two departments, and be communicated and implemented at all levels as soon as possible.	Enterprise-wide accountabilities for privacy and security will be formalized from the Deputy Ministers to individual employees. An all-encompassing privacy statement that summarizes, for clients and staff, the Department's commitment for the proper handling of their personal information, will be enunciated.	Second quarter of fiscal year 2004-05	DG, Corporate Communications Directorate (HRSDC) DG, Corporate and Ministerial Affairs (SDC)
2) Policies and procedures on the management of personal information should be reviewed to ensure the coverage of the privacy components is adequate and sufficient.	As a component of the Privacy Management Framework, and with the assistance of privacy and security expertise, Branches will be mandated to review the adequacy and sufficiency of their policies and procedures for the management of personal information. As required, Branches will modify policy and procedures, based on this review, to ensure that coverage of privacy components is adequate and sufficient.	First quarter of fiscal year 2004-05	DG, Corporate Communications Directorate (HRSDC) DG, Corporate and Ministerial Affairs (SDC)
3) Agreements signed by teleworkers should be standardized to ensure that the clauses dealing with the confidentiality of personal information are specific on the obligation to protect the confidentiality of the information and the rules that must be followed. Members of EI board of Referees should be required to sign a similar agreement.	Review consistent application of teleworker agreements for employees and take steps to standardize Agreements, where necessary. Policy and procedures, to ensure Board of Referee members are advised of and agree to the obligation to protect the confidentiality of the information in appeal dockets/hearings/ decisions, will be developed and implemented, with the Commissioner's approval.	October, 2004 October 1, 2004	DG, Human Resources Programs Directorate DG, Insurance Policy

**Updated August 2004*

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
4) A national strategic communication and training plan should be developed to ensure that all employees who have access to personal information receive timely and adequate training and information on the legislation, policies, and procedures for the use and protection of personal information in their area of activities.	Phase I – Research to assess learning needs, define learning objectives and identify gaps Phase II – Design and/or adaptation of learning products to identify the best approach, methodology and learning tools to meet the learning objective. Phase III – Implementation to deliver training materials to certified trainers and work with other branches and regions to implement a "train the trainer" approach. Training by FAS Security.	September 30, 2004 October 30, 2004 December 31, 2004 On-going	DG, Human Resources Programs Directorate DG, Administrative Services
5) Management should ensure that those who give and are given access to personal information understand the nature and application of the "need-to-know" principle and the consequences of violations such as "browsing" and unlawful disclosures.	EI (Employment Insurance) actions are addressed in recommendation No. 9 ISP (Income Security Program): • System Access Control Position; • Review current User ID/user profiles in Legacy System to ensure accuracy and up-to-date; • Implementation of the National Operational Guidelines for Requesting Access (Job Profiles); • Map access rights from ISP Legacy System to ISP Delivery Systems; • Review and update ISP User Access Guide/Entry-Exit procedures. Departmental Accounts Receivable Systems (DARS): • Ensure that the job descriptions and associated security matrix properly aligned with the information available; • Review of the screens associated with the elements in the security matrix; • Based on the outcomes of the above review ,defining revised business requirement will be undertaken to develop a revised security matrix, if required; • Impact assessment of these changes will have on existing policies for operational guidelines will be conducted; • All new DARS users will receive a document on the legislation, policies and procedures for the use and protection of personal information.	Second quarter of fiscal year 2004-05 Second quarter of fiscal year 2004-05 Second quarter of fiscal year 2004-05 NHQ: On-going as functionality increases, project finish 2007 Annual Review September 30, 2004 March 31, 2005 September 20, 2005 Completed Completed	DG, Strategic Integration, ISP DG, Accounting Services

**Updated August 2004*

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
6) All situations where public companies are used to ship or destroy material that contains personal information should be covered by a contract that establishes and specifies the responsibility of the company to protect the confidentiality of the information while under its control. Only the last three digits of the Social Insurance Number should be indicated on the boxes sent to National Archives.	Liaise with Privacy to confirm applicable clause to be used and with PWGSC. Develop and implement procedures and communicate to regional procurement officers and privacy coordinators. Guidelines have been amended to advise that only the last three-digit-unit of the SIN should be written on the box exteriors that are being shipped or stored outside HRSDC/SDC.	December 2004 December 2004 Completed	DG, Administrative Services
7) Given the wide variety of situations calling for the protection of the confidentiality of client files, it is recommended that HRSDC and SDC conduct individual risk and control assessment in premises where documents containing personal information are stored to determine if the level of protection against unauthorized access or withdrawal of client files is adequate.	Several Threat and Risk Assessment (TRA) will be conducted throughout the department and the necessary control procedures are taken as result of TRAs. Security sweeps will be augmented as well as security awareness sessions.	To cover entire department for the fiscal year 2004-05.	DG, Administrative Services
8) The rules and procedures for recording the source and the reason for changes to personal information and for keeping evidence documents should be clarified to reduce the risk of inappropriate changes that may cause hardship.	EI Program to issue national directive to clarify policies and procedures for documenting source and reason of change.	September 2004	DG, Insurance Policy

**Updated August 2004*

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
9) For all the persons involved in the process of management of all User IDs and profiles providing access to personal information, responsibility and accountability should be clearly defined and implemented Documentation should be available on the nature of the personal information the employee is given access to.	Completion of all EI national job profiles (75% currently profiled) EI program manager's roles, responsibility and accountability for profiles and user codes defined. Implementation of job profiles ISP will update on a regular basis the user, management and Systems Access & Control Officer (SACO) roles and distribute the SACO User Guide. Develop a document which clearly defines the roles of individuals involved in establishing a user code in Departmental Accounts Receivable System (DARS).	Completed Second quarter 2004-05 See response by Systems Branch in recommendation No.11 October 2004 September 30, 2004	DG, Insurance Services DG, Strategic Integration, ISP DG, Accounting Services
10) Accountability and responsibility for the attribution of User ID that meet the privacy requirements should be defined, understood and accepted.	IT/Security Operations will define and communicate all the roles and responsibilities for all the steps in the attribution, maintenance and suspension of the User ID. Guidelines will be developed in consultation with Regional access coordinator with respect to annual reviews and cancellation of user codes for Departmental Accounts Receivable System (DARS).	First draft September 2004 September 30, 2004	Senior DG, Technology Services Directorate Senior DG, Information Technology Operations DG, Accounting Services

**Updated August 2004*

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
11) To allow effective and efficient monitor access to personal information, and to facilitate periodic audits, the following should be created as soon as possible:			
1. A list of all the User IDs that provide access to EI, ISP or FAS (DARS) programs and databases containing personal information, certified by the proper level of authority (to be identified in the Privacy Accountability Framework presently underway);	IT Operations/Security will produce a report to be verified by RC managers within all program areas. This report will display User ID, name, PRI and access capabilities to which program areas this User ID has authorized access. ISP will develop and implement a National Report to RC managers. The program authorities will limit access within their program area.	September 2004 Anticipated implementation September 2004.	Senior DG, Technology Services Directorate ISP Strategic Information Directorate RC Managers
2 Practical processes to determine with certainty the identity of the incumbent of each of the User IDs listed in (1)	The activities listed above will result in the verification of the usability of all User IDs and the incumbent. To ensure that information stays accurate and timely, the following options are being explored: a. automatic suspension of inactive User ID; b. interface to FAS Security to ensure being advised of changes in employee's status; and c. Quarterly review/updates with all RC managers.	October 2004	Senior DG, Technology Services Directorate
3. Practical processes to determine with certainty the function exercised by each incumbent identified in (2)	The activities listed as responses to recommendations #11; items 1 and 2 will identify and verify the access capabilities of the employee. The program areas determine the functions that can be exercised within the program area through management response to recommendation No. 9	Timeline for recommendation #9 and then additional 3 months to identify each user's profile and then matching these profiles to User ID.	SDG/ TSD, SDG/ITO Program areas
4. Grids linking each function identified in (3) to an access profile that meets privacy requirements.	Once the program areas complete creation of profiles (groups of transactions codes) then ITO/Security will create a corresponding profile within Security Management and Single Logon (SMSL). The program areas will identify profiles to each user. ITO/Security will match the profile to the User ID. Reports to be circulated to RC managers for verification	Timeline for recommendation #9 and then additional 3 months to identify each user's profile and then matching these profiles to User ID.	SDG/ TSD, SDG/ITO Program areas
	EI: • Develop and implement approval process for granting access to EI data (NHQ requests);	Completed	DG, Insurance Services

**Updated August 2004*

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
	• Develop approval process for granting access to EI data (Regional requests);	Second quarter 2004-05	
	• Implement Regional EI Approval process;	To be determined in consultation with the regions	
	• Develop monitoring process to ensure effective management of user codes in conjunction with ITC Security. To be part of overall Systems' plan to review existing documentation, procedures and processes addressed in recommendation No. 10.	To be determined in consultation with ITC Security	
	ISP actions ensuring business requirement for access:		
	• Obtain user list; • Align Users to existing organizational structure; • Map delegations of authority to work descriptions; • Map work descriptions to access; • Management review and approval; and • SACO updates user list.	On-going as functionality increases, projected completion 2007	DG, Strategic Integration, ISP
	DARS:		
	• Develop a list of all Users IDs for DARS.	Completed	DG, Accounting Services
	• Cross reference the name of each individual with access to DARS by PRI.	September 2004	
	• Require the entry of an individual PRI before issuing a User ID.	Completed	
	• Establish a security matrix based on job function for DARS.	Completed	
	• Establish a security matrix incorporating the job descriptions. Further ensure that edits are in DARS which prohibit the creation of a user profile with an invalid security matrix combination.	Completed	

**Updated August 2004*

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE	RESPONSIBILITY
Protected			

INTERNAL AUDIT RECOMMENDATIONS	CORRECTIVE MANAGEMENT ACTION PLAN	EXPECTED COMPLETED DATE*	RESPONSIBILITY
13) The Information Designation / Classification Guide should be supplemented with guidelines that would provide practical guidance on the classification and handling of the documents containing personal information most frequently used by the various programs. Internal controls should be put in place to ensure that protected material is handled according to its level.	Produce a manual/guide that will assist employees on the handling, classifying, transmitting and storing of classified and sensitive information. Update security awareness training, including safeguarding sensitive information. Resume security sweeps.	Completed Completed	DG, Administrative Services
14) The process to be followed by managers and employees who become aware of a possible privacy violation should be clarified and communicated.	Provide a departmental manual on Guidelines for Conducting Administrative Investigations. Conduct awareness sessions on the application of the process for conducting administrative investigations with stakeholders (i.e. HRS, Legal and Security).	Completed Fiscal year 2004-05	DG, Administrative Services
15) The nature and sensitivity of the information disclosed should be taken into account in the distinction between formal and informal disclosure and the rules for documenting the disclosure should be reviewed. The rules and procedures for recording the source and the reason for informal disclosure of personal information should be clarified.	The existing training material used by ISP, NHQ will be examined to ensure that the issue of recording the release of sensitive information in response to informal requests, namely verbal inquiries, is emphasized with employees. Branches will also be asked to review their procedures, as they relate to recording verbal informal releases of information.	Third quarter fiscal year 2004-05	DG, Corporate Communications Directorate (HRSDC) DG, Corporate and Ministerial Affairs (SDC)

**Updated August 2004*

APPENDIX C: LIST OF OFFICES VISITED

LIST OF OFFICES VISITED			
BC	1	PC ISP	Victoria
	2	PC/HRCC EI	Victoria
	3	ISP Telecenter	Vancouver
	4	IPOC	Vancouver
		RHQ	Vancouver
	5	DARS	Vancouver
SK	6	HRCC/PC EI	Regina
	7	EI Telecenter	Regina
	8	DARS	Regina
		RHQ	Regina
	9	PC ISP	Winnipeg
		ITC	Winnipeg
PEI	10	PC EI	Montague
	11	HRCC EI	Charlottetown
	12	PC ISP	Charlottetown
		RHQ	Charlottetown
NB	13	EI Telecenter	Bathurst
	14	ISP Telecenter	Bathurst
	15	PC EI	Bathurst
	16	DARS	Moncton
	17	IPOC	Moncton
		ITC	Moncton
	18	PC ISP	Fredericton
		RHQ	Fredericton
ON	19	PC ISP	Chatham
	20	HRCC/PC	St.Catherines
	21	Satellite	Niagara Falls
	22	HRCC/PC	Mississauga
	23	EI Telecenter	Toronto
	24	ISP Telecenter/PC	Scarborough
		RHQ (ISP)	Toronto
		ITC	Belleville
	25	IPOC	Belleville
	26	DARS	Belleville
		RHQ (EI)	Belleville

LIST OF OFFICES VISITED			
QC	27	PC ISP	Québec
	28	Satellite	Québec
	29	PC EI	Sherbrooke
	30	PC EI	Montréal
	31	DARS	Montréal
		ITC	Montréal
	32	EI Telecenter	Montréal
	33	ISP Telecenter	Montréal
	34	IPOC	Montréal
		RHQ	Montréal
Total:		34 Offices 6 RHQs 4 ITCs	
Audit NHQ		EI FAS ISP SP Systems	(DARS, Security, Privacy, Administrative Services, Legal Services)