Correctional Service Canada | Service correctionnel Canada

SAFETY, RESPECT AND DIGNITY FOR ALL

LA SÉCURITÉ, LA DIGNITÉ ET LE RESPECT POUR TOUS

# PRIVACY AUDIT

Internal Audit Branch

378-1-204

Final – October 2006

Canada

## Table of Contents

# EXECUTIVE SUMMARY

The audit of privacy was conducted as part of CSC's internal audit plan for 2005-2006. The verification phase of this audit was performed during the months of November and December 2005 at which time the audit team visited the five regional headquarters and two institutions per region.

The objectives established for the audit were as follows:

- To assess the management framework in place with respect to privacy.
- To determine the extent to which proactive measures are taken to identify and investigate potential and actual privacy breaches and that corrective actions are taken.
- To determine the extent to which appropriate processes and procedures are in place to obtain informed consent from offenders with respect to the disclosure of health information.
- To determine the extent to which procedures are being followed to support the timely processing of privacy requests.

In order to assess the above objectives, the audit team examined key policy and training documents relating to privacy as well as relevant reporting and monitoring systems. Staff at the national, regional and local levels were interviewed, as well as offenders. The audit also collected data regarding the processing of privacy requests and examined a sample of files on the Offender Management System to determine the extent of health care information contained in various case management reports.

**Conclusions**

The results of this audit have indicated that the current management framework for privacy addresses certain roles and responsibilities and provides direction on specific aspects of privacy within CSC. However, there are gaps in the framework that need to be addressed.

The audit further identified a concern regarding a general lack of understanding amongst staff of what constitutes a real or potential privacy breach. During site visits, the audit team found several examples of common practices that did not ensure the protection of employee or offender personal information. There is a need for increased training or awareness in this regard.

Implementation of the recommendations contained in this report will contribute to CSC's adherence to central agency legislation and policy requirements. More detailed conclusions for each audit objective are outlined below.

**Management Framework**

The audit found that the management framework for privacy within CSC is fragmented, leading to gaps and, in some cases, unclear direction. Several sectors within NHQ are all working in some way to meet CSC's obligations, however, there is no overall coordination.

The audit further found that those directly responsible for privacy matters (eg., NHQ ATIP staff or Regional and local Privacy coordinators) clearly understand their roles and responsibilities with respect to privacy. However, many staff outside of these areas at all levels of the organization seem unaware of the potential privacy implications of certain practices, including the potential risk in the event of disclosure or loss of information. This was evident during site visits both through observation and interviews.

Finally, local, regional and national processes have not been clearly defined and communicated to ensure that potential and confirmed privacy breaches are identified and reported through key organizational authorities.

**Investigations and Corrective Action**

While the audit found that some breaches are being investigated, the process is not consistently applied and clear direction is lacking at the national level.

The audit team further concluded that effort is being made by some divisions at NHQ to distribute period reminders and disseminate information about potential privacy breaches and problems along with lessons learned, however, the ATIP Division, does not currently share national data, results and analyses regarding privacy breaches or lessons learned with the staff at the regional, institutional or community level. As a result, it reduces CSC's ability to avoid the occurrence of similar breaches within the organization.

**Offender Consent and Confidentiality of Health Care Information**

Health care staff at the institutions visited were following appropriate processes and procedures to ensure that informed consent is obtained from offenders prior to disclosing health related information. Offender health information collected and controlled by Health Care was well managed and staff were aware of the requirements as dictated by professional standards.

There is a need, however, for CSC to review the health care information collected during the Preliminary Assessment and Immediate Needs Interviews in order to determine its relevance to the intake assessment process and the need for recording such health care information on OMS. Also, further guidance should be provided to community and institutional Parole Officers regarding the need for informed consent when offenders are self-disclosing health information to ensure that all privacy requirements are respected.

In terms of the consent forms being used, while there were no concerns with respect to the offenders' understanding of these forms, the audit found that many institutions had created in-

house forms in order to address provincial and professional requirements. In this regard, CSC must ensure there is a consistent and efficient approach to amending the consent forms used in the institutions to ensure that these forms remain up-to-date and contain all necessary clauses.

**Timeliness of the Processing of Privacy Requests**

CSC has made progress to improve the timeliness of responses to privacy requests. However, while processes, procedures, and monitoring tools are understood and being used, the volume of requests results in staff at all levels of the organization not always being able to comply with the 30 day timeframe. Current resourcing levels and methods for retrieval and shipping of information often prevent the timely processing of requests.

Recommendations have been made in the report to address the issues identified. A management action plan has been prepared and included in Annex D.

# 1.0 INTRODUCTION

The Privacy Act came into effect in Canada on July 1, 1983. The Act:

- protects the privacy of individuals with respect to personal information about themselves where it is held by a federal government institution; and
- provides individuals with the right of access to their personal information and correction to such information.

According to the Act, individuals have certain rights with respect to the personal information that is maintained by the Correctional Service of Canada (CSC), specifically:

- To know what personal information is collected about them by government institutions and why the information is collected.
- To know how that personal information is used, who has access to it and for what purpose.
- To know what personal information is kept by institutions of the federal government, how long it is kept and how it is ultimately disposed.
- To request that any personal information about them that is used to make a decision that affects them directly be corrected if it is not accurate, up to date or complete.
- To file a complaint to the Privacy Commissioner of Canada.

The Privacy Act also created the Office of the Privacy Commissioner (OPC). The Commissioner is an ombudsman appointed by Parliament to investigate complaints relating to requesting or obtaining access to personal information under the Act.

In addition to the Privacy Act, CSC has issued a number of Commissioner's Directives which pertain to the protection of private information. As privacy touches on many of the operational areas in CSC (including security, informatics, records management, human resources management, health services, etc) there are several related to CSC's obligations under the Privacy Act.

Within the Correctional Service of Canada, there is an Access to Information and Privacy (ATIP) Division. It is the focal point for the application of the Access to Information Act and the Privacy Act, which has been delegated the full authority to exercise the powers and perform the duties and functions of the Minister under the Privacy Act. The Division reports to the Director General, Rights, Redress and Resolution who in turn reports to the Assistant Commissioner, Policy and Research. "The ATIP Division deals directly with the public in connection with ATIP requests and serves as the centre of ATIP expertise in enabling CSC to meet its statutory obligations under the Acts. To that end, the Division is responsible for ensuring that formal access and privacy requests are completed in a timely manner, and for promoting a culture of openness and accountability while ensuring that safe and appropriate safe guards are respected with regards to all personal information."[1]

[1] ATIP InfoNet site, http://infonet/corp_dev/rights_redress_resolution/atip/about_rrr_atip_e.shtml

On average, the Correctional Service of Canada receives 5,500 privacy requests annual from offenders and approximately 500 requests from CSC staff. For fiscal year 2003-2004, as a result of requests submitted in bulk from Correctional Officers and offenders, CSC received 19,829 requests. Bulk requests also increased the number of privacy requests received in 2004 – 2005 and carried over from the previous year to 16,770. The NHQ ATIP Division works within a budget of just under $2,100,000 which allows for an indeterminate staff of 37 employees. Of these, 22 employees are responsible for the vetting of all requests flowing through the ATIP office, including both Privacy and Access to Information requests.

To understand the concerns associated with CSC's privacy program, preliminary discussions were conducted with the Privacy Commissioner's Office and Correctional Investigator's Office, as well as subject matter specialists within CSC such as the ATIP Division, Health Care Services, Information Management Services, and the Security Division. The following section outlines the key concerns identified during the audit planning process.

i. Privacy Complaints (files with the Office of the Privacy Commissioner)

In the 2005-2006 Annual Report to Parliament, the Privacy Commissioner cites CSC as having received the highest number of complaints pertaining to privacy requests, with a total of 190 complaints between April 2005 and March 2006. This number includes all complaints including access (108), privacy (39) and time limits (43) (refer to Annex A for definitions). While the report notes that those institutions which hold a large amount of personal information (such as CSC) are more likely to receive complaints, the report goes on to further break down these findings. Of the 120 investigations which the Office of the Privacy Commissioner closed during the 2005-2006 year relating to access and privacy, CSC was found to have 17 "well founded"[2] complaints. Of these, approximately half were related to access and the rest to the use and disclosure of personal information such as:

- An employee photo being improperly used;
- Information discovered by an inmate in the recycling bin; and
- Disclosure of offender information to the wrong offender.

ii. Timeliness of Responses to Privacy Requests

For the last several years, in its Annual Report to Parliament, the Office of the Privacy Commissioner has cited the Correctional Service for not responding to privacy requests within legislated timeframes. In the 2005-2006 Report, the Office of the Privacy Commissioner reported that of the 61 investigated complaints against CSC regarding timeliness, 89% were well-founded. This would include complaints from staff, offenders and members of the public. In relation to other departments, CSC has the second highest percentage of well-founded complaints regarding timeliness.

[2] As per the Office of the Privacy Commissioner well-founded means "the government institution failed to respect the *Privacy Act* rights of an individual". Office of the Privacy Commissioner, Annual Report to Parliament 2005-2006, http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.asp#015

Despite CSC increasing its ATIP staff and streamlining its procedures, delays in responding to requests for personal information continues. The ATIP Division at NHQ took special measures to reduce the backlog of overdue privacy requests in the first four months of 2005. The result was that current late requests (other than those from Correctional Officers, but including bulk offender requests) were reduced from more than 1250 to 150. Although the ATIP Division is committed to maintaining a 90 –100% compliance level with respect to legislative time frames, this is proving to be problematic. Concern exists that a backlog of privacy requests could once again become an issue.

iii. Privacy Breaches

In preparing for this audit, a review was conducted of the types of privacy incidences that had occurred during 2004-2005 and had been reported through the ATIP Division at NHQ. The majority of incidences reported involved the loss, misplacement or mishandling of hard copy files, laptops and computer disks. The other significant reported trends involved the accidental sharing or misdirection of personal information, primarily relating to offenders, but also to employees and others.

In July 2005, the ATIP Division, in cooperation with Departmental Security Division, distributed a document designed to clarify the procedures to be followed in reporting potential as well as confirmed privacy breaches and encouraged pro-active initiatives aimed at minimizing the risk of future privacy breaches occurring. This document is entitled, *Privacy Breaches: A Guide for Regional and Institutional Managers*.

iv. Offender Consent and Confidentiality of Health Care Information

The Office of the Correctional Investigator (OCI) has raised concerns about offenders being provided with informed consent prior to sharing medical and mental health information. The OCI also raised a concern about the confidentiality of offender health information and the potential for inappropriate medical and mental health care information to find its way into Offender Management System (OMS) records.

*a) Informed consent*

In his 2003-2004 annual report, the Correctional Investigator identified reservations about the clarity of the consent forms offenders are signing. He questioned whether the technical and/or legal wordings of the forms are beyond the reading level and comprehension of most offenders. In interviews with staff of the OCI, the concern raised was that some national consent forms are too “all inclusive” and may request the offender’s blanket consent to disclosing all information for risk assessment purposes. This could be interpreted as an infringement upon their privacy rights. Staff of the OCI were also aware that some operational facilities had produced their own in-house consent forms. They questioned whether the locally-produced forms respected legal and professional requirements around the issue of “informed consent”.

The Health Services Branch of CSC concur that consent forms should make it clear that only information related to risk or its management will be passed on to non-health care professionals

involved in the case and that other information will be kept private in accordance with relevant legislation and professional standards. The national consent forms, in combination with direction provided by health care professionals are designed to meet the requirements of informed consent.

In CSC's response to the CI's report, it was stated that "an internal audit focussing on privacy of information will be conducted … and will include the issue of confidentiality of health information".

b) *Disclosure of confidential health information*

CSC Policy currently states that offender medical information will be shared only with the offender's consent. When an offender consents to psychiatric or psychological assessment/treatment for case management purposes the offender also consents to the sharing of relevant information with the case management team. In addition, this policy requires that information being shared without consent is done on a need-to know basis, is documented, and the offender will be informed of the disclosure unless it jeopardizes the safety of any person. In their 2003-2004 Annual report, the Correctional Investigator expressed concerns regarding the disclosure of confidential health information and the extent to which staff have a "need to know" confidential offender health information.

For CSC Health Services, the issue raised by the CI is one of balance. Health care providers have a dual mandate: to protect the confidentiality of offender health information while also providing sufficient and relevant information to case managers and other decision makers to allow them to manage risk. In other words, it is not necessary to share every detail of an offender's medical diagnosis or condition in order for case managers and decision makers to be properly informed. Health Services is of the opinion that the current policies in place at CSC prevent the unnecessary disclosure of offender health information.

## 2.0 AUDIT OBJECTIVES AND SCOPE

### 2.1 AUDIT OBJECTIVES

The objectives of the audit were:

- To assess the management framework with respect to privacy.
- To determine the extent to which proactive measures are taken to identify and investigate potential and actual privacy breaches and that corrective actions are taken.
- To determine the extent to which appropriate processes and procedures are in place to obtain informed consent from offenders with respect to the disclosure of health information.
- To determine the extent to which procedures are being followed to support the timely processing of privacy requests.

The third objective was specifically examined in response to concerns expressed by the Correctional Investigator in his 2003-2004 annual report.

The specific criteria used for the audit can be found in Appendix B.

### 2.2 AUDIT SCOPE

The audit was national in scope, and the audit work was conducted at ten (10) of CSC's 54 institutions in all five regions and five (5) Regional Headquarters (RHQ) as well as at National Headquarters (NHQ). Site selection for the ten sites visited took place in consultation with relevant Offices of Primary Interest at NHQ based on the following:

- Security level;
- Frequency of audit activity at sites;
- OPI input; and
- Geographic location.

A list of the sites visited can be found in Appendix C.

The scope of the audit did not include community offices. In addition, the audit did not examine the access controls over information contained in the Offender Management System (OMS) or other information systems such as the Human Resource Management System (HRMS).

## 3.0 APPROACH AND METHODOLOGY

Prior to site visits, an audit program was developed and preliminary testing of the tools took place at one site in the Ontario region. The site visits were conducted in November and December of 2005. They consisted of direct observation of potential or evident privacy breaches, documentation reviews, offender file reviews, and interviews with offenders and key staff members.

Audit teams were composed of one Internal Audit Branch staff member, as well as a Privacy Coordinator and Medical Health Care professional.

Documents reviewed on a national basis included the ATIP Compliance Manual; various Commissioner's Directives; the Privacy Breach Guide; Offender Orientation / Information Manuals; Management Control Framework attestations with respect to Consent to Health Care Services; documentation for staff training, orientation, and awareness sessions on privacy requirements; and offender consent forms in use at the institutions. Documents reviewed specific to the institutions visited include any institutional based communications giving staff members direction on privacy issues, as well as any information pertaining to complaints received with respect to privacy breaches. Using a review period of November 2004 – November 2005 the audit team examined offender medical and psychological files to ensure the necessary consent forms were included. A random sample of 10 files was reviewed at each site, with the requirement that the review include 5 medical files and 5 psychological files. The audit

team also reviewed the corresponding Offender Management System files to verify that only appropriate medical or mental health care information was included in reports used for risk assessment and decision making purposes.

At the institutional level, interviews were held with a variety of managers and staff such as the Assistant Warden Management Services, Chief of Administrative Services, Institutional Privacy Coordinators (where available), Records Assistants, Chiefs of Informatics, Chiefs of Human Resources, Coordinator of Correctional Operations, and Main Receptionists (where available). The purpose of these interviews were to determine the extent to which the Privacy Breach Guide had been implemented and what if any economies or efficiencies could be brought to the issue of timely processing of privacy requests. Institutional interviews were also conducted with the chiefs of Health Care and Psychology as well as institutional nurses, psychologists and offenders. The purpose of these interviews was determine how informed consent was managed in an operational setting and if any issues around offender confidentiality of medical and mental health care information were evident.

At the regional level, managers responsible for privacy, records management, informatics, security, health care and human resources were interviewed to determine what privacy issues were being experienced at this level.

The audit also incorporated direct observation at all sites visited in order to identify potential breaches and determine the extent to which personal employee and offender information was being managed and protected.

Following completion of site visits, preliminary findings were shared with senior managers at the site and regional levels through debriefings. Once all visits and interviews at the regional and national level were completed, debriefings were also held with representatives of the Policy and Research Sector, as well as Correctional Operations and Programs (including Health Care), Human Resource Management and Corporate Services.

# 4.0 FINDINGS AND RECOMMENDATIONS

## 4.1 MANAGEMENT FRAMEWORK

**Objective 1: To assess the management framework in place with respect to privacy.**

With respect to the management framework, the audit team expected that corporate accountabilities and responsibilities at National Headquarters (NHQ), Regional Headquarters (RHQ) and operational facilities would be defined; integrated policies, guidelines and procedures on the handling of personal information would be documented and easily accessible. The audit team also expected that awareness and training sessions would have been conducted in relation to privacy issues as well as the handling of personal information; and monitoring and reporting mechanisms would be in place at NHQ, RHQ and operational facilities to control the risk associated with potential or confirmed privacy breaches.

### 4.1.1 Corporate accountabilities and responsibilities

**Finding: Corporate accountabilities and responsibilities for privacy among NHQ Sectors are not comprehensively defined.**

The audit team found that the ATIP Compliance Manual (dated November 2003) provides information concerning the accountability framework for privacy. With respect to accountabilities, the manual touches upon the delegation of authority for key positions such as the Minister, Commissioner, Senior Deputy Commissioner, the Assistant Commissioner responsible for ATIP (the Assistant Commissioner, Policy and Research) as well as the Regional Deputy Commissioners, Wardens, District Directors and some other designated positions within the regions.

A review of corporate documentation on the CSC Infonet and discussions with NHQ managers revealed that there are sectors at National Headquarters other than Policy and Research that have key mandates and responsibilities which impact the accountability framework of ATIP and the *Privacy Act*, but are not identified in the ATIP Compliance Manual. These include:

- Corporate Services: Information Management Systems (IMS) and Records Management are large collectors, users and protectors of personal and / or protected information, relating to both employees and offenders;
- Correctional Operations and Programs (COP): Security, Reintegration and Health Care Services are responsible for significant amounts of personal and protected offender information;
- Human Resource Management (HRM): is responsible for the Human Resource Management System database which contains personal employee information. This Sector is also responsible for the National Training Standards (NTS) (which includes training modules on ATIP) as well as *Commissioner's Directive (CD) 060* entitled the *Code of Discipline* (which deals with employees who intentionally misuse or mishandle personal or protected information).

As discussed under section 4.1.4 below, some of these divisions have also established monitoring systems to identify, control and report upon privacy breaches.

Overall, the audit team found that the accountability framework needs improvement, particularly with respect to the identification and integration of privacy accountabilities and responsibilities of Sectors such as Corporate Services, Correctional Operations and Programs and Human Resource Management. Overall, various sectors are working on different aspects of privacy in relative isolation with no overall coordination. The risk of not having a comprehensive and integrated accountability framework is that there may be gaps or overlaps in responsibilities. Further, in a decentralized organization such as the Correctional Service of Canada, the ability to identify and correct program obstacles is inhibited. Similarly, opportunities for program enhancements may not be recognized.

**Finding: Privacy Coordinators at the regional and local levels clearly understand their roles and responsibilities.**

The audit found that each region had identified a Regional Privacy Coordinator, however, the classification of this position varied from one region to the other (ranging from AS-02 to AS-05). In three regions, the position is located in the Executive Services division, however, in the Atlantic and Quebec regions, it falls under Corporate Services.

At the local level, each institution visited had assigned the duties of privacy coordination to a staff member as part of other duties. In most cases, this was the Chief of Administrative Services. This person is also responsible for other key activities such as offender complaints and grievances, claims against the Crown, records management, etc.

With respect to privacy, Coordinators at the regional and local levels are responsible for duties such as:

- coordinating and processing requests (ensuring legislated timeframes are met);
- at the regional level, processing requests from offenders who have reached their Warrant Expiry Date (i.e., no longer under the jurisdiction of CSC);
- informal sharing of information with offenders and staff as applicable; and
- participating in the reporting process for privacy breaches.

In addition, both regional and local Privacy Coordinators process requests from outside organizations such as police organizations, provincial governments, courts, etc. This task is highly sensitive as it relates to the sharing of offender personal information outside of CSC and requires a high level of knowledge of the Privacy Act and the Corrections and Conditional Release Act (CCRA).

Interviews with Coordinators at the regional and local levels did not identify any major issues with respect to the understanding of their roles and responsibilities. Issues raised related more to the volume of work and the fact that privacy was only one of several priorities under their responsibility.

### 4.1.2 Corporate policy framework

**Finding: A policy framework for privacy exists, however, it is fragmented and in need of improvement.**

The audit team found a number of Commissioner's Directives (CD), Guidelines and Standard Operating Practices (SOPs) which cited the *Privacy Act* as an authority or provided guidance on some privacy-related matter. Although not an exhaustive list, the following identifies the types of policy documents found on the CSC Infonet which included a privacy component:

- CD-226 – Use of Electronic Networks;
- CD-095 and Guidelines - Information Sharing with Offenders;
- SOP-700-01 - Information Sharing and Disclosure;
- CD-803 - Consent to Health Service Assessment, Treatment and Release of Information;
- CD-850 - Mental Health Services;
- CD-568 - Management of Security Information;
- CD-568-6 – Creation, Control and Handing of Preventive Security Files; and
- CD-060 - Code of Discipline.

Each of these policies touches on a specific aspect of privacy or discusses certain responsibilities regarding the protection of personal information.

In addition to the above-noted corporate policy documents, the audit team identified two other documents related to privacy:

a) ATIP Compliance Manual

The ATIP Compliance Manual (dated November 2003) is available to all staff via the CSC Infonet. It contains a variety of information, including:

- accountabilities, roles and responsibilities;
- program-related information including legal authorities under the Privacy Act; and
- a step-by-step guide to the processes and procedures to be followed when requesting and processing privacy requests.

Although the ATIP Compliance Manual provides a considerable amount of information concerning the privacy program, it contains many references and citations which are now out-of-date. Additionally, the link to Chapter 4 (entitled "Guide for the Use and Disclosure of Personal Information about Offenders") indicates that this will be added at a later date. As of August, 2006, Chapter 4 had still not been included in the Compliance Manual on the Infonet.

b) Privacy Breach Guide

The Breach Guide is a brief PowerPoint presentation entitled "Privacy Breaches – A guide for regional and institutional managers". It was distributed nationally in July 2005 and posted on CSC's Infonet in February 2006. The Breach Guide provides a brief overview of definitions,

responsibilities, and steps to be followed in the event of a potential or confirmed privacy breach, as well as direction regarding investigations and steps to be followed once a privacy breach is discovered.

**Finding: The direction contained in the Privacy Breach Guide is limited and unclear.**

The audit team found limitations with the Breach Guide from a policy perspective. First, its presentation as a PowerPoint document is informal. As a corporate document providing national direction on the management and prevention of privacy breaches, the Breach Guide should be presented in a recognized policy format.

In addition, the audit team found the Privacy Breach Guide to be incomplete and unclear in many areas. Similar concerns were also expressed during interviews with institutional and regional staff. Examples of issues identified include:

- There is no reference to the handling of privacy breaches at National Headquarters or within the community (District, Parole Office or Community Residential Facility);
- Certain positions cited in the Guide do not exist (eg., Regional Administrator, ATIP);
- A number of terms (eg., fact finding investigation, threat and impact assessment) are not clearly defined in the Guide nor understood by those interviewed;
- The emphasis in the Privacy Breach Guide is directed towards security breaches, however, passing reference is given to records management and informatics. There are many other types of potential privacy breaches which do not fall under these headings;
- The investigative and reporting processes were not clear to those interviewed who are responsible for implementing the Guide. In addition, certain elements do not agree with the flowchart available on the Infonet entitled “Breaches of Privacy and/or Government Security Policy - Mandatory Reporting Protocol”;
- The Privacy Breach Guide states that “Unless clearly unnecessary, a fact-finding investigation of the breach must be convened at the institution”. The Guide is not clear on what type of privacy breach would require no review process.

The Guide currently applies the same reporting and investigative processes to all types of breaches, however, revisions to the Guide could consider different levels of investigation depending on the degree of risk and impact of the breach.

Finally, the audit found that the Privacy Breach Guide provides little guidance with respect to corrective measures, rather it focuses on the administrative processes to follow if a breach is identified.

Overall, the audit team found that the Privacy Breach Guide does attempt to provide some direction; however, clarification is required on a number of issues in order to ensure a consistent application across CSC.

### 4.1.3 Training and awareness

**Finding: Some training modules are being delivered with respect to privacy, however, it is evident that staff are not clear as to what constitutes a potential or actual privacy breach.**

At the national level, the audit team identified various documents used for training purposes relating to Disclosure of Personal Information, Privacy Impact Assessments, Overview of the ATIP Compliance Manual, and Overview to the Access to Information and Privacy Act for Managers. These documents are used by the ATIP Division in various orientation sessions delivered at the Correctional Management Learning Centre and for some ad hoc training in the regions.

As part of the National Training Standards (NTS), other orientation modules which include a privacy component have been developed such as: New Employee Orientation Program (NEOP); Correctional Officer Training (CTP); and Orientation for Assistant and Deputy Wardens. In addition, a scan of the sector Infonet sites revealed a number of PowerPoint presentations produced by Information Management Systems and Information Technology (Corporate Services) as well as the Security Division (Correctional Operations and Programs) related to the protection of CSC personal and protected information and assets with a focus on privacy.

The Privacy Breach Guide states that ATIP, with the assistance of the Security Branch, will provide training on the Breach Guide. The audit team was advised, however, that no training had been conducted either prior to or following national distribution of the Breach Guide. At the time of the audit, no training modules on the Breach Guide had been developed and no training schedule had been established. Many staff interviewed at the regional and local levels were unaware of the guide or were unfamiliar with its content.

At the local level, the audit team confirmed that some institutions visited had conducted awareness sessions at venues such as staff assemblies and a few examples were found where e-mails were sent to staff reminding them of their obligations with respect to the care and protection of personal and protected information. The audit team found no information to support that any training or awareness sessions had been conducted by the regions.

The audit found that there are varying degrees of understanding about the management and handling of personal information. During visual inspections at ten institutions and five regional headquarters, the audit team identified a number of privacy concerns including:

- Count boards with information such as offenders' names and Finger Print Sheet (FPS) numbers, cell numbers, appointments with outside court and hospital visits clearly visible to offenders or visitors to the institution;
- Photographs of offenders with their names and FPS numbers were posted in the main entrance at one institution;
- At another institution, there was a board at the front desk that held visitors' personal identification (such as a driver's licence) which had been exchanged for a CSC visitor's

pass. The personal identification was clearly displayed such that others could view not only the name of the visitor but their picture and other personal information as well.

- Filing cabinets containing personal and protected information with no locking mechanisms;
- Lists containing personal information posted outside of offices;
- Sensitive / confidential information left unattended for long periods of time (eg., overnight or during periods of leave); and
- Limited security and control over boxes containing protected / confidential information intended for shredding.

When these were brought to the attention of privacy staff and institutional and regional managers, they indicated that they did not recognize these to be potential breaches of privacy.

There is a risk that the lack of formal training and awareness relating to privacy issues is resulting in breaches occurring but not being recognized, reported or addressed.

### 4.1.4 Corporate monitoring and reporting mechanisms

**Finding: A number of corporate monitoring and reporting mechanisms exist to capture breaches that may have privacy implications, however there is limited integration and analysis of the information.**

A number of corporate systems have been established to monitor and report on breaches which have privacy implications. For example,

- security breaches are reported through a network called SINTREP (managed by the Correctional Operations and Programs Sector);
- breaches in the information technology systems within CSC such as the Offender Management System (OMS) are monitored and reported upon by a group within Information Management System (IMS) (Corporate Services Sector);
- Records Management uses protocols established by the Offender Records System (ORS) to manage potential and/or confirmed breaches associated with the loss, destruction or mishandling of hard copy files (Corporate Services Sector); and
- the ATIP Division has established a system to record potential and confirmed privacy breaches reported by regions and institutions based upon direction provided in the Privacy Breach Guide (Policy and Research Sector).

The audit team found that there was no coordination between or integration of the various monitoring systems that have been established within CSC to identify and report upon privacy breaches. These different monitoring systems gather information about various elements of breaches occurring; many of which have privacy implications. However, there is no single corporate location where a comprehensive picture of the scope of privacy breaches can be examined. In addition, there is no analysis being done as to the more common types of privacy breaches occurring and possible means of avoiding them.

The current monitoring and tracking systems are highly dependent upon the various Divisions being advised by staff at NHQ, or in the regions, institutions and districts when a recognized privacy breach occurs. The audit team found, however, that there was a genuine lack of clarity as to what actually constituted a privacy breach and to whom it should be reported. For example, a misplaced or mishandled offender file could have multiple breach implications for security, records management, and privacy. Clarity around what constitutes a reportable privacy breach is required. In many cases, the scope of the breaches of personal and protected information crosses various responsibility centres and sectors making it unclear as to what monitoring and reporting system should be used to track the breach.

**CONCLUSION**

The audit found that the management framework for privacy within CSC is fragmented, leading to gaps and, in some cases, unclear direction. Several sectors within NHQ are all working in some way to meet CSC's obligations, however, there is no overall coordination.

The audit further found that those directly responsible for privacy matters (eg., NHQ ATIP staff or Regional and local Privacy coordinators) clearly understand their roles and responsibilities with respect to privacy. However, many staff outside of these areas at all levels of the organization seem unaware of the potential privacy implications of certain practices, including the potential risk in the event of disclosure or loss of information. This was evident during site visits both through observation and interviews.

Finally, local, regional and national processes have not been clearly defined and communicated to ensure that potential and confirmed privacy breaches are identified and reported through key organizational authorities.

**Recommendation 1: The Assistant Commissioner Policy and Research should work closely with other senior managers to develop a comprehensive accountability framework for privacy activities within CSC.**

**Recommendation 2: The Assistant Commissioner, Policy and Research should ensure that the policy framework for privacy (including the Privacy Breach Guide) is better integrated and provides clear and consistent direction.**

**Recommendation 3: The Assistant Commissioner Policy and Research (in consultation with the Assistant Commissioner Corporate Services and the Assistant Commissioner Correctional Operations and Programs) should review the current reporting and monitoring systems to clearly define the reporting requirements and ensure a consolidation and analysis of the information.**

**Recommendation 4: The Assistant Commissioner, Policy and Research, in consultation with the Assistant Commissioner, Human Resource Management, should develop and implement a national strategic communication and training plan with respect to the protection of personal information, as well as the required investigative and reporting processes.**

## 4.2 INVESTIGATIONS AND CORRECTIVE ACTION

**Objective 2: To determine the extent to which proactive measures are taken to identify and investigate potential and actual privacy breaches and that corrective actions are taken.**

The expectation for this objective was that a process was in place to ensure that breaches are investigated and that corrective measures had been implemented. We also expected to find some communication mechanism in place to ensure that lessons learned were being corporately shared.

It should be noted that the results identified under the first objective (management and policy framework) are clearly linked to the audit findings for this second objective. Given a lack of awareness regarding what constitutes a privacy breach, a lack of understanding regarding the investigative and reporting process and gaps in accountabilities (roles and responsibilities), the audit team was unable to assess compliance with many aspects of the program. Overall, the audit found that many requirements are not being followed or are inconsistently applied, however, this is largely due to different interpretations and understanding of the requirements. The recommendations made under the first objective should assist in clarifying these issues and in improving compliance.

The following sections touch on a small number of other specific issues relating to this objective that have not already been addressed elsewhere in this report.

### 4.2.1 Breach investigations and corrective measures

**Finding: The audit found that investigations are being conducted as a result of certain breaches, however the application and format is inconsistent.**

The audit team found that investigations are being done for certain types of breaches, particularly those with a significant impact (eg., loss of laptop or offender file or personal information being accessed by offenders). Various formats and distribution were found with respect to these investigations, due in large part to the lack of clear direction in this regard as previously identified under objective 1.

In addition, given that staff were unclear as to what constitutes a privacy breach, there is no assurance that all breaches are being reported, investigated and addressed.

With respect to corrective action, the audit found that there is no current means to report or track what is being done to address issues identified during privacy breach investigations. While the audit found that disciplinary action was taken in some cases as a result of investigations, this was managed locally and was not necessarily reported as part of the privacy process.

### 4.2.2 Lessons learned

**Finding: Some information about lessons learned was found on the CSC's Infonet.**

The audit team expected to find that information disseminating from breach investigations would be acted upon in order to prevent similar incidents from occurring in other areas of CSC.

The audit team was unable to obtain verification that lessons learned are corporately disseminated by the ATIP Division. During interviews with ATIP officials it was explained that the Division receives information about privacy breaches, however, they do not prepare or disseminate periodic analyses of lessons learned. Similarly, while the ATIP Division prepares summaries for senior management of breaches reported in the Office of the Privacy Commissioner's Annual Report to Parliament, this information is also not shared with the regions or institutions. A review of the 82 breaches reported to the ATIP Division during the 2005-2006 fiscal year highlights several recurring types of breaches, such as personal information being left in recycling bins and found by offenders (in one institution, three such breaches were reported in three separate months).

The audit team found that general information has been prepared by the IMS Branch on the protection of Information Technology (IT) information and assets, however, during interviews, few Privacy Coordinators in the regions and institutions were aware of this information. Information prepared by the Departmental Security Division, such as security bulletins on the Government Security Policy were also found on the CSC Infonet. Security staff interviewed at the regional and institutional level knew about this information, however, few Privacy Coordinators were aware of this resource.

The audit team notes that the ATIP Division recently posted a document entitled "ATIP-Tips" on the CSC Infonet. This publication (dated November 2005 and posted on CSC's Infonet in February 2006) focuses on the legislative and legal scope and authority of the Privacy Act. Interviews revealed that future editions of ATIP-Tips may include information about lessons learned and ways to avoid potential privacy breaches.

**CONCLUSION**

While the audit found that some breaches are being investigated, the process is not consistently applied and there is a lack of clear direction from the national level. Further, as noted previously, staff are unaware of privacy implications of certain practices, thus a number of privacy breaches are not being reported and are therefore not being investigated or addressed.

The audit team further concluded that effort is being made by some divisions at NHQ to distribute period reminders and disseminate information about potential privacy breaches and problems along with lessons learned, however, the ATIP Division, does not currently share national data, results and analyses regarding privacy breaches or lessons learned with the staff at the regional, institutional or community level. As a result, it reduces CSC's ability to avoid the occurrence of similar breaches within the organization.

**Recommendation 5: The Assistant Commissioner, Policy and Research should ensure that key information is shared at the appropriate levels such as lessons learned and examples of common privacy breaches in order to minimize the risk of further breaches occurring.**

## 4.3 CONSENT AND CONFIDENTIALITY OF OFFENDER HEALTH CARE INFORMATION

**Objective 3: To determine the extent to which appropriate processes and procedures are in place to obtain informed consent from offenders with respect to the disclosure of health information.**

As per CD 803, *Consent to Health Services, Assessment, Treatment and Release of Information*, offenders must sign consent forms for all medical and mental health procedures, for involvement in research, as well as for the sharing of his/her health care information. This consent must be informed, meaning that the offender has the capacity to understand and is made aware of the possible results and risks. The audit team expected to find that protocols are in place to ensure that offenders are properly informed of what they are consenting to, that consent forms are clearly understood by offenders, and these forms take into account all aspects of legislated requirements. The audit team also expected to find that health care professionals have been trained and/or provided with an awareness of the requirements relating to informed consent.

CSC policy requires that offender consent must be obtained for the sharing of health care information, except under certain circumstances. The exceptions include:

- where the information is relevant to the decision to release the offender,
- there is reason to believe the offender poses a serious threat to himself or the safety of the institution, and/or
- disclosure is mandated or permitted by relevant legislation (e.g. the *Corrections and Conditional Release Act*, the *Privacy Act*, provincial legislation regarding the reporting of communicable diseases, etc.).

In addition to these requirements, this information may only be shared with those staff members who have a "need to know". As a result, the audit team expected to find only necessary health care information on the case management files reviewed.

### 4.3.1 Protocols for informed consent

**Finding: While there is no formal protocol in place regarding informed consent, consistent procedures were generally being followed by all sites visited.**

Health care professionals at all of the sites visited had a complete understanding of the concept of informed consent. Though protocols and procedures may differ slightly between sites, protocols may generally be described as:

- Providing the offender with the blank consent form;
- Providing the offender with a verbal explanation of the blank consent form;
- Providing the offender with a verbal explanation of the procedure, treatment, or assessment being proposed and any applicable issues regarding the disclosure of information as applicable;
- Verbal responses to any offender questions or concerns; and
- Completion of the consent form prior to health services being provided.

No concerns were noted in this area.

### 4.3.2 Training/awareness of informed consent

**Finding: While CSC has not provided specific training and/or awareness sessions on informed consent, training has been provided to CSC health care providers through their professional certification and licensing.**

No concerns were noted in this area. Professional and licensing requirements dictate that medical and mental health care providers provide informed consent including the disclosure of health care information. The audit found that while no training is available within CSC to address this issue, CSC staff working in health services have the required knowledge base as a result of information and/or training acquired through their respective professional organizations as is it a standard of practice for health care practitioners.

### 4.3.3 Consent forms

**Finding: Consent forms are generally understood by offenders.**

Offenders were interviewed at each of the sites visited, either individually or in a group setting, regarding whether the consent forms are clear. In all cases, offenders stated that the consent forms used by CSC are comparable to what may be found in the community setting and are understood. The offenders also noted that if a situation arises where they do not understand the written form, health care staff will take whatever time is necessary to explain the areas that are not clear.

No concerns were noted in this area.

**Finding: Institutions have created in-house consent forms in order to address provincial legislative and professional requirements.**

The audit team reviewed a sample of consent forms being used in minimum, medium, and maximum security institutions. Although CSC has created national generic forms, these often do not reflect the specific professional and legislative requirements that vary between provinces. In order to address this issue, many institutions have added to the generic forms and created their own in-house forms which take into account the provincial requirements.

While the audit did not include a detailed examination of the content of these amended forms, a risk was noted given their diversity. A cursory review of a small sample of forms noted issues such as: in-house forms not being available in both official languages or not using the same wording or statement of consent that is found in the official form.

Interviewees at the institutions visited were not aware whether any of the locally created consent forms had been reviewed by CSC Legal Services and/or RHQ Health Care to verify that all requirements have been met. When NHQ Health Services was consulted, they noted that they are aware that a number of different consent forms exist in the institutions, however they have not completed a review of any of these forms.

The creation of in-house forms may have legal ramifications as CSC could be liable should any necessary clause in the consent form be unintentionally removed or amended.

### 4.3.4 Disclosure of offender health information

**Finding: Offender Management System files reviewed contained only health care information reasonably related to risk assessment, with the exception of Preliminary Assessments and Immediate Needs Interviews.**

In reviewing the offender files on the Offender Management System (OMS), the audit team did not find offender health care information being recorded in Correctional Plan Progress Reports, Case Work Records or Assessment for Decision reports unless reasonably related to risk assessments.

The audit team noted, however, that the Preliminary Assessments and Immediate Needs Interviews contain health care information for every offender.

The Preliminary Assessment is used to collect basic data on the offender, assess his or her immediate needs, initiate the collection of the critical documents and orient the offender to the CSC. Preliminary Assessment interviews are normally held within 5 working days of the offender receiving a federal sentence (eg., while the offender is still in the custody of provincial authorities) and are conducted by a Community Parole Officer. All information collected during this process is entered into the OMS.

In addition, CSC policy requires that an Immediate Needs Interview be conducted by the Institutional Parole Officer within one working day of the offender's arrival. The policy states that the purpose of the Immediate Needs Interview is to confirm information acquired through the Preliminary Assessment and enter alerts/flags/needs into OMS as required. The results of the interview are recorded in a Casework Record on OMS.

Content requirements for both interviews include information related to the offender’s basic status (eg., marital, language, citizenship, offence, sentence, etc.) as well as medical needs (eg., medication, allergies), mental health needs (eg., history of treatment), security needs (eg., gang affiliation, incompatibles), and suicide risk (eg., previous attempts, recent intervention).

The following issues were noted with respect to this process:

- use of the information - from a health care perspective, interviewees reported that while policy requires that all offenders are seen by a Nurse within two working days of initial reception, in most cases, the practice is to see all offenders upon their arrival in the admissions area before they are assigned to a cell. Many interviewees in Health Care stated that they did not have access to OMS therefore the information collected during the Preliminary Assessment or Immediate Needs Interview was not reviewed by them. Rather, the source of key information is the medical file provided by the local or provincial authorities.

- informed consent - Although there is specific direction that health services may not share information without informed consent, there is no guidance as to whether or not this consent is required for self-disclosed information from the inmate during the Preliminary Assessment. In addition, there is no evidence that first-time offenders are made aware that the information provided for the Preliminary Assessment or Initial Interview will be recorded in OMS.

- accuracy of the self-disclosed information - The Institutional and Community Parole Officers responsible for collecting this information have not received health care training and therefore may have more difficulty understanding or assessing the completeness or accuracy of information provided by offenders. There is no evidence that the information provided by the offender is confirmed or modified by Health Care following their evaluation. As offenders' OMS records follow them throughout their sentence, there is a potential that inaccurate health care information may be used by staff members.

From a privacy perspective, this information becomes accessible to individuals who may not have a "need to know". In addition, it is being recorded without the evidence of necessary consent and the potential exists for inaccurate health information may be used by staff members in making decisions without it being properly validated through Health Services.

## CONCLUSION

Health care staff at the institutions visited were following appropriate processes and procedures to ensure that informed consent is obtained from offenders prior to disclosing health related information. Offender health information collected and controlled by Health Care was well managed and staff were aware of the requirements as dictated by professional standards.

There is a need, however, for CSC to review the health care information collected during the Preliminary Assessment and Immediate Needs Interviews in order to determine its relevance to the process and the need for recording such health care information on OMS. Also, further guidance should be provided to community and institutional Parole Officers regarding the need for informed consent when offenders are self-disclosing health information to ensure that all privacy requirements are respected.

Finally, as the legislated and professional requirements for consent change frequently and vary between provinces, CSC must ensure there is a consistent and efficient approach to amending the consent forms used in the institutions to ensure that these forms remain up-to-date and contain all necessary clauses.

**Recommendation 6: The Assistant Commissioner Correctional Operations and Programs should examine the offender health information collected during the Preliminary Assessment and Immediate Needs Interview processes, in order to determine the best approach and provide necessary guidance.**

**Recommendation 7: The Assistant Commissioner Correctional Operations and Programs should ensure that all locally-developed consent forms are reviewed for consistency, legality and applicability.**

## 4.4 TIMELINESS OF THE PROCESSING OF PRIVACY REQUESTS

**Objective 4: To determine the extent to which appropriate procedures are being followed to support the timely processing of privacy requests.**

In the effort to respond to privacy requests in a timely manner it is important that CSC implement procedures to facilitate this process. The audit team expected to find that appropriate procedures have been outlined and are being followed to support the timely processing of privacy requests. As per the Privacy Act, CSC has 30 calendar days to respond to privacy requests. This timeline starts from the day the privacy request is received, and the completed package must be sent to the requester by the 30th day.

The audit team expected to find that legislated timeframes are being respected for all privacy requests. The audit team also expected to find monitoring systems in place to ensure that CSC is meeting legislated timeframes. Should these systems identify specific issues in the area of timeliness, the audit team expected that delays are being addressed.

### 4.4.1 Processes and procedures

**Finding: Procedures for the processing of privacy requests have been established in the ATIP Compliance Manual, and they are generally understood and followed by Privacy Coordinators.**

The NHQ ATIP Sector has produced an ATIP Compliance Manual which outlines the processes and procedures to be completed by each level of CSC (i.e. national, regional, and local, depending on the request) when processing privacy requests. The 30 day process translates in to 20 working days for all of the steps to be completed. As per the ATIP Compliance Manual, the following chart outlines the steps in the process, the number of days allocated for each, as well as the area of CSC responsible at each interval:

| Time Allocated | Steps | Number of Days Used |
|---|---|---|
| **1 day** (ATIP) | Receipt of the request / Clarification of request, as required | 1 |
| **1 day** (ATIP) | Entry in ATIP tracking system (ATIPflow) and submission of retrieval notice by e-mail. | 2 |
| **7 days** (NHQ / REGION / OPERATIONAL UNIT) | Search and retrieve (+ numbering and photocopying) all relevant records, including the receipt of these in the ATIP Division. | 9 |
| **5 days** (ATIP) | Review of the records / Consultation process, as required. | 14 |
| **2 days** (ATIP) | Second review process. | 16 |
| **2 days** (ATIP) | Preparation of release package, including removing information withheld from disclosure within the package. | 18 |
| **1 day** (ATIP) | Approval and signature by the delegated authority. | 19 |
| **1 day** (ATIP) | Mail-out of the release package. | 20 |

The Manual also contains details regarding what each step in the process requires. The audit team found that the ATIP Compliance Manual is generally understood and followed by the Privacy Coordinators at the institutions visited. Although the procedures are easily understood, the amount of time it takes to actually complete the process has been identified as an issue, which will be addressed in the next section.

### 4.4.2 Timeliness of requests

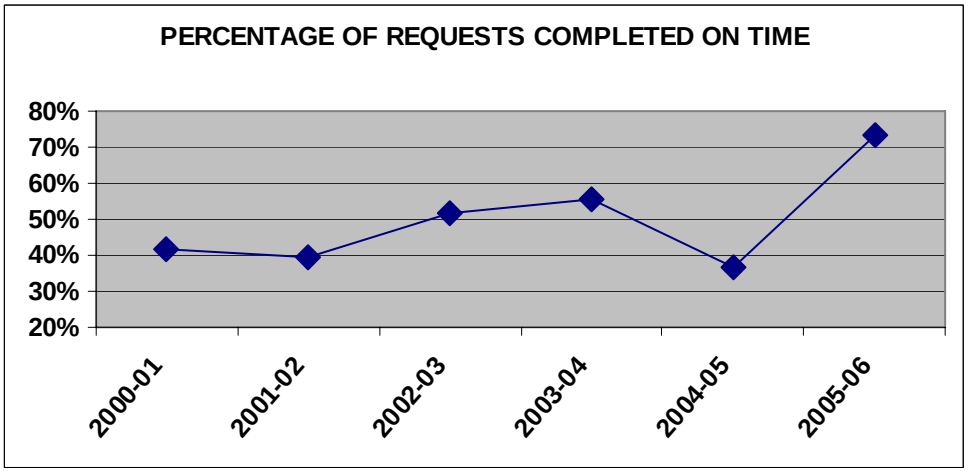
**Finding: While staff members are complying with processes identified in the ATIP Manual, they are not always able to meet the legislated 30 day timeframe.**

Once institutions have gathered all relevant documentation, the packages are sent to NHQ ATIP for review and vetting. The large number of requests received influences the timeliness of CSC's responses. As per the most recent organizational chart for the NHQ ATIP Sector, there are currently 22 Information Analysts employed at NHQ. These 22 positions are responsible for the vetting of all privacy requests received across the organization.

The total number of privacy requests received by CSC as well as the number of completed requests is tracked by the NHQ ATIP Sector. The audit team requested these numbers for the past six fiscal years. The following charts illustrate the total number of requests received as well as the percentage of requests which were completed on time:

| FISCAL YEAR | TOTAL NUMBER OF PRIVACY REQUESTS RECEIVED |
|---|---|
| 2005-2006 | 7,783 |
| 2004-2005 | 15,812 |
| 2003-2004 | 19,829 |
| 2002-2003 | 5,899 |
| 2001-2002 | 6,110 |
| 2000-2001 | 4,042 |

*Information provided by NHQ ATIP, 2006-07-12




*Information provided by NHQ ATIP, 2006-07-12

As can be seen from this graph, CSC has made progress to improve the timeliness of responses to privacy requests, however is still unable to fully comply with the legislated timeframes. The reasoning for late responses was questioned at the institutions visited and at NHQ ATIP. While some of these institutions were able to meet the timeframes for privacy requests, there were typically lower security/smaller facilities where the institution receives significantly fewer privacy requests. The smaller sites visited during the audit were also more likely to share information informally with offenders. In addition, privacy requests in the lower security level facilities typically involve fewer pages. As there are fewer requests involving fewer pages, processing places less of a burden on the resources of the institution and the ability of staff to meet timeframes.

Those institutions visited which were unable to meet the legislated timeframes were mostly larger institutions of a higher security level. Of the institutions where a large number of overdue requests were found, the most common reasons for the extended timeframes include:

- Offenders at higher security levels tend to make more requests for litigious reasons and privacy requests at these institutions often involve a larger number of pages;
- The quality of photocopiers (i.e. photocopiers breakdown or jam regularly, are not high speed and/or high resolution) and access to these copiers is often an issue;
- In one region, there are limitations with respect to mail and courier services (centralized via a regional depot) which impact on the individual institutions' ability to meet the established timeframes.

- The method used to collect, number, and copy files is extremely time consuming and labour intensive;
- There is often a lack of trained resources available to meet privacy deadlines (due to absence or other operational demands) and the retention of trained clerical staff is a concern in many institutions.

It should be noted that none of institutions are funded for positions to respond to ATIP requests. As previously mentioned, Privacy Coordination duties have been assigned to existing positions as one of many responsibilities.

While the Privacy Act does provide for a maximum 30 day extension, these circumstances are specific. This includes cases where

- meeting the timeframes unreasonably interferes with the operations of the department,
- consultations are required that cannot reasonably be completed within the original time limit,
- translation is required, or
- information must be converted into an alternate form.

These reasons for extension, however, often cannot be used by CSC. In the case of timeframes unreasonably interfering with the operations of the department, this may only be applied when bulk requests are received in one area of operations (for example when a large number of requests are received at the same institution). As requests are most often received from various sites across CSC, the extension would not apply.

As per the report provided by NHQ ATIP, the following table outlines requests received, completed on-time, as well as the number of overdue requests for FY 2005-06:

**Privacy Requests for Fiscal Year 2005-2006**

| | |
|---|---|
| **Requests completed on time** | 5,699 |
| **# of days completed after due date:** | |
| 1 – 30 days | 1,164 |
| 31 – 60 days | 301 |
| 61 – 90 days | 131 |
| 91 – 120 days | 77 |
| Over 120 days | 411 |
| **Total overdue** | 2,084 |
| | |
| **Total requests** | 7,783 |

*Information provided by NHQ ATIP, 2006-07-12

Though clear processes and procedures have been outlined, the large volume of requests makes it difficult for all requests to be competed on time using the current method of retrieval and review. At this time, by not meeting the 30 day timeframes, CSC is not complying with the Privacy Act.

### 4.4.3 Monitoring of timeliness

**Finding: All sites visited as well as the ATIP Division at NHQ have implemented systems to monitor timeframes for processing privacy requests.**

The institutions and Regional Headquarters are responsible for the gathering of all pertinent documents related to the privacy request. All of the institutions and Regional Headquarters offices visited had established a log for tracking the due date for these documents to reach the NHQ ATIP office. These tracking systems varied from the use of computer programs to hand written notes.

At the National level, ATIP uses the ATIPFlow program to monitor all steps in the privacy request process. This includes the date the request was received, the final due date, when the record retrieval notice is sent to the institution or RHQ, any reminders that have been sent to the sites when documents are not received on time, and at which step in the process the file rests. As the documents become overdue from the institutions or Regional Headquarters, a memo is sent notifying the site that the records must be shipped to NHQ immediately.

Although these monitoring systems are in place, files continue to be completed beyond the due date for the reasons identified in section 4.4.2. Attempts have been made to resolve the issues related to delays. For example, in cases where bulk requests are made from the same site, additional resources are used to hire casual help and rent additional photocopiers to help process these requests as quickly as possible. While these additional resources help, they are only temporary and the original backlog of requests remains.

**CONCLUSION**

CSC has made progress to improve the timeliness of responses to privacy requests. However, while processes, procedures, and monitoring tools are understood and being used, the volume of requests results in staff at all levels of the organization not always being able to comply with the 30 day timeframe. Current resourcing levels and methods for retrieval and shipping of information often prevent the timely processing of requests. The issue of timely response to privacy requests is important because by not adhering to the legislated timeframes, CSC is not in compliance with the law.

**Recommendation #8: The Assistant Commissioner Policy and Research should review the current situation to determine the best approach to meeting legislated timeframes.**

# 5.0 GENERAL CONCLUSION

The results of this audit have indicated that the current management framework for privacy addresses certain roles and responsibilities and provides direction on specific aspects of privacy within CSC. However, there are gaps in the framework that need to be addressed. A key factor is the fact that there are currently many different sectors / branches at NHQ working in isolation on related issues with no overall coordination or communication.

Roles and responsibilities of those directly involved in privacy matters at the national, regional and local levels were well-understood, however, the audit identified a concern regarding a general lack of understanding amongst staff of what constitutes an actual or potential privacy breach. During site visits, the audit team found several examples of common practices that did not ensure the protection of employee or offender personal information. There is a need for increased training or awareness in this regard and roles and responsibilities need to be clarified, particularly with respect to the reporting and investigative processes.

While the focus of the audit was on the overall privacy program, two specific aspects were examined in further detail. With respect to the issue of informed consent and the offenders' understanding of consent forms, the audit identified no major concerns. However, there is a need to clarify requirements regarding health care information collected during the Preliminary Assessment and Immediate Needs Interview and ensure a review process is in place for any in-house forms created.

Finally, the audit found that while the number of requests processed on time has improved, CSC is still not meeting the legislated timeframes in this regard.

# Appendix A – Definitions of Complaint Types

Complaints received in the Office are categorized into three main groups:

**Access:**

- **Access –** All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.
- **Correction/Notation –** The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.
- **Language –** Personal information was not provided in the official language of choice.
- **Fee –** Fees have been assessed to respond to a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.
- **Index –** Infosource [1] does not adequately describe the personal information holdings of an institution.

**Privacy:**

- **Collection –** Personal information collected is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.
- **Retention and Disposal –** Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in Infosource): either destroyed too soon or kept too long.

  In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.

- **Use and Disclosure –** Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible disclosures without consent listed in section 8(2) of the *Act*.

**Time Limits:**

- **Time Limits –** The institution did not respond within the statutory limits.
- **Extension Notice –** The institution did not provide an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.
- **Correction/Notation - Time Limits –** The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

Source: Office of the Privacy Commissioner, Annual Report to Parliament 2005-2006, http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.asp#015

# Appendix B – Objectives and Criteria

| Objective | Criteria |
|---|---|
| **Objective 1:**<br>To assess the management framework in place with respect to privacy. | **Criteria:**<br>1.1 Accountabilities have been clearly established at NHQ, RHQ, and in operational facilities.<br>1.2 Policies, guidelines and procedures are in place with respect to privacy.<br>1.3 Awareness sessions and/or training has been conducted with respect to privacy.<br>1.4 Monitoring and reporting mechanisms are in place at NHQ, RHQ, and operational facilities to ensure that the risk of privacy breaches is minimized. |
| **Objective 2:**<br>To determine the extent to which proactive measures are taken to identify and investigate potential and actual privacy breaches and that corrective actions are taken. | **Criteria:**<br>2.1 Mechanisms are in place to ensure that breaches are investigated and corrective action is taken to address privacy breaches and related issues.<br>2.2 Lessons learned are corporately disseminated to ensure that similar breaches do not occur. |
| **Objective 3:**<br>To determine the extent to which appropriate processes and procedures are in place to obtain informed consent from offenders with respect to the disclosure of health information. | **Criteria:**<br>3.1 Protocols are in place to ensure that offenders are properly informed of privacy protections and limitations with respect to disclosing of health information.<br>3.2 Health Care providers have been provided with adequate training and/or awareness with respect to informed consent.<br>3.3 Consent forms are clear and comprehensible to offenders and are consistent with relevant policy and legislation.<br>3.4 Offender case management files contain only necessary health care information. |
| **Objective 4:**<br>To determine the extent to which appropriate procedures are being followed to support the timely processing of privacy requests. | **Criteria:**<br>4.1 Privacy procedures are in place that conform to the ATIP Compliance Manual and ensure the efficient processing of requests.<br>4.2 Staff comply with legislated time frames and overall guidelines in processing privacy requests.<br>4.3 There is a system in place to monitor timeframes to ensure that they are met, and ensure issues related to delays are addressed. |

Note: The third objective was specifically examined in response to concerns expressed by the Correctional Investigator in his 2003-2004 annual report.

# Appendix C – Sites Visited

**Atlantic Region:**

Westmorland Institution

Springhill Institution

Regional Headquarters

**Quebec Region:**

Federal Training Centre

Leclerc Institution

Regional Headquarters

**Ontario Region:**

Millhaven Institution

Pittsburgh Institution

Regional Headquarters

*Note: Collins Bay Institution served as the test site.*

**Prairies Region:**

Regional Psychiatric Centre

Riverbend Institution

Regional Headquarters

**Pacific Region:**

Pacific Institution

Mountain Institution

Regional Headquarters

# Appendix D – Management Action Plans

| Recommendations | Primary Responsibility | Action Plan | Target completion date |
|---|---|---|---|
| **Recommendation 1: The Assistant Commissioner Policy and Research should work closely with other senior managers to develop a comprehensive accountability framework for privacy activities within CSC.** | ACPR | • Prepare, for EXCOM approval, a Privacy Management Framework (PMF) setting out accountabilities for protection of privacy, management of privacy breaches and building a culture of compliance with the Privacy Act and Treasury Board Policies on privacy ( to include a communications strategy and evaluation framework)<br>- review existing departmental and Privacy Commission models and prepare a draft outline - September 30, 2006<br>- consultation with Sectors and Regions - December 31 2006<br>- final framework presented to EXCOM – March 31, 2007<br>- | March 31, 2007 |
| **Recommendation 2: The Assistant Commissioner, Policy and Research should ensure that the policy framework for privacy (including the Privacy Breach Guide) is better integrated and provides clear and consistent direction.** | ACPR | • Prepare, for EXCOM approval, a Policy on interactions between ATIP and CSC partner Sectors and Regions, which outlines expectations on collaboration regarding ATIP Requests, privacy protection and ATIP-related policies. (include communications strategy and evaluation framework)<br>- draft completed<br>- consultation of Regions and Sectors – December 31 2006<br>- present to EXCOM – March 31, 2007<br>• Elaborate procedures governing interactions between ATIP and specific CSC partners on subjects related to the function of each partner (include communications plans and evaluation provisions)<br>- draft complete<br>- consultation with CSC partners – December 31, 2006<br>- present to EXCOM – March 31, 2007<br>• Review and finalize a draft policy on management of privacy breaches for EXCOM approval (including communications strategy and evaluation framework)<br>- re-draft of procedure complete<br>- consult with Departmental Security Division –October 15, 2006<br>- consult with Regions and Sectors – December 31, 2006<br>- present to EXCOM – March 31, 2007 | March 31, 2007 |

| Recommendations | Primary Responsibility | Action Plan | Target completion date |
|---|---|---|---|
| **Recommendation 3: The Assistant Commissioner Policy and Research (in consultation with the Assistant Commissioner Corporate Services and the Assistant Commissioner Correctional Operations and Programs) should review the current reporting and monitoring systems to clearly define the reporting requirements and ensure a consolidation and analysis of the information.** | ACPR | • Consult CSC experts and OPI's to identify sources of breach information and potential for integrated electronic reporting – December 31, 2006<br>• Plan and implement new applications to permit access and reporting – June 30, 2007<br>• Evaluate effectiveness – March 31, 2008 | March 31, 2008 |
| **Recommendation 4: The Assistant Commissioner, Policy and Research, in consultation with the Assistant Commissioner, Human Resource Management, should develop and implement a national strategic communication and training plan with respect to the protection of personal information, as well as the required investigative and reporting processes.** | ACPR | • In consultation with DG Learning and Development, identify training and information objectives and performance indicators – December 31, 2006<br>• Identify and design appropriate and cost-effective courses and learning tools – March 31, 2007<br>• Pilot and consult on approaches – September 30, 2007<br>• Implement – March 31, 2008 | March 31, 2008 |
| **Recommendation 5: The Assistant Commissioner, Policy and Research should ensure that key information is shared at the appropriate levels such as lessons learned and examples of common privacy breaches in order to minimize the risk of further breaches occurring.** | ACPR | • Identify key information and types of information according to potential impact in reducing numbers and impact of breaches – October 31, 2006<br>• Identify the recipients of key information who will most effectively implement necessary changes – December 31, 2006<br>• Design and pilot the most effective tools for communicating key information – February 28, 2007<br>• Evaluate, adjust and implement –March 31, 2007 | March 31, 2007 |
| **Recommendation 6: The Assistant Commissioner Correctional Operations** | ACCOP | In Aug 06 ACCOP directed that a working group be established to review the Preliminary Assessment and Immediate Needs Interview | June 30, 2007 |

| Recommendations | Primary Responsibility | Action Plan | Target completion date |
|---|---|---|---|
| **and Programs should examine the offender health information collected during the Preliminary Assessment and Immediate Needs Interview processes, in order to determine the best approach and provide necessary guidance.** | | process to determine the most effective approach to achieve efficiencies including if needed proposed policy changes. | |
| **Recommendation 7: The Assistant Commissioner Correctional Operations and Programs should ensure that all locally-developed consent forms are reviewed for consistency, legality and applicability.** | ACCOP | Health Services in concert with Legal Services will review all health-related forms currently in use and develop a format which is deemed the most appropriate (e.g. generic or Regional forms). | March 31, 2007 |
| **Recommendation #8: The Assistant Commissioner Policy and Research should review the current situation to determine the best approach to meeting legislated timeframes.** | ACPR | The Division has already undertaken a number of initiatives geared to increase the effectiveness and timeliness of our retrieval and analysis functions, including:<br>• Implementation of a knowledge management tool to provide ad hoc references and precedents to analysts<br>• Conclusion of a series of agreements with Prairie Region to pilot more efficient methods of accessing files from the Region and of providing disclosure in an informal, routine and formal fashion<br>• Implementation of best practice requirements to ensure quality and consistency of analysis within the Division<br>• Identification of needed electronic tools and application (e.g. ATIPImage) to reduce paper-driven tasks<br>• Enhanced training of Regional Administrators and provision of periodic information and training bulletins to CSC staff on relevant issues<br>• Development of a competency-based staffing procedure to ensure continuity and professional development of staff<br><br>These improvements will be considered within our process of further identifying means of improving effectiveness as follows:<br>• Gather all relevant current surveys and | June 30, 2008 |

| Recommendations | Primary Responsibility | Action Plan | Target completion date |
|---|---|---|---|
| | | analyses prepared by ATIP or similar Divisions in other Departments and jurisdictions - complete<br>• Plan (including timing, resourcing and methodology) other necessary analysis of points at which delays occur, and causes of these – October 31, 2006<br>• Identify the most cost-effective solutions (human resources, techniques, procedures, tools, operational management) – March 31, 2007<br>• Determine resource needs and seek resources inside, and then outside, the Division – May 31, 2007<br>• Present to EXCOM – September30, 2007<br>• Pilot – December 31, 2007<br>• Evaluate and implement final measures – June 30, 2008 | |