Correctional Service Canada Service correctionnel Canada

Safety, Respect and Dignity for All

La sécurité, la dignité et le respect pour tous

Audit of Safeguarding of Physical Offender and Staff Records

Internal Audit

378-1-253

April 13, 2010

Canada

Table of Contents

EXECUTIVE SUMMARY

As outlined in its 2009-2010 Report on Plans and Priorities, CSC has established five priorities in response to the changing offender profile. One of the identified priorities is the "*safety and security of staff and offenders in our institutions*".

CSC employs 15,400 employees, of which approximately 85% work in either an institution or in the community. Furthermore, CSC is responsible for approximately 13,500 incarcerated offenders[1]. The Service is responsible for the proper creation, management and safeguarding of offender and staff records. Offender records contain personal and other sensitive information on an offender's background, criminal history, health, and case management while in the custody of CSC. Staff records may also contain potentially sensitive personal information. It is important for the Service to ensure that there is appropriate safeguarding of records to reduce safety and security risks to staff and offenders in institutions.

As part of the risk-based audit planning process, an audit in this area was identified for fiscal year 2009-2010 and the objectives were:

- To provide reasonable assurance that the management framework in place supports the effective safeguarding of physical offender and staff records; and
- To provide assurance that CSC is in compliance with the various legal and policy requirements related to the safeguarding of physical offender and staff records.

In order to conclude on the above objectives, the audit team reviewed the overall framework in place with regards to the safeguarding of both offender and staff records. The audit team reviewed legislation, key policies and procedure manuals, examined both offender and staff files, and carried out visual inspections in 17 institutions and 3 Regional Headquarters. In addition, a total of 103 interviews were conducted with staff in various positions within the institutions and with staff at both Regional and National Headquarters.

Overall Conclusion

Key elements of a management framework are in place to support the safeguarding of offender records. CSC policies and user guides are consistent with relevant legislation and with government policies. Procedures and manuals are comprehensive and generally well understood by staff. Some training tools exist and mechanisms are in place to report and manage privacy breaches.

Nonetheless, our audit showed that attention is required in the following areas:

[1] Reports on Plans and Priorities – 2009-10

- There is a need for direction, guidance and clarification of corporate roles and responsibilities with respect to the management and safeguarding of physical staff records;
- Roles and responsibilities with respect to the management of physical offender and staff records should be fully documented;
- Training should be enhanced; and
- Monitoring and reporting is focused mainly on privacy breaches and could be improved.

While we found many practices that comply with the various safeguarding requirements related to the classification, filing, maintenance, access, movement, storage and disposal of records, we also noted areas of non-compliance as follows:

- Some documentation in files, primarily observation reports, printed e-mails and documents created by third parties, are not being marked as Protected when necessary;
- There are several instances where staff files were not well maintained, including several documents not being affixed to the folder;
- Shadow and temporary files are being used within many institutions and offices;
- Documents given to offenders by CSC are not always properly identified;
- File jackets are not always signed or annotated when individuals access an offender file;
- The “need to know” principle is not always well applied, specifically with regards to access by staff of offender personal information;
- There are gaps in the safeguarding of the offender records in transit within and/or between institutions;
- Files, including in some cases Preventive Security records, are not always stored appropriately based on the sensitivity and protection level of the documentation; and
- Protected information is not always being disposed of appropriately.

Recommendations have been made in the report to address these areas for improvement. Management has reviewed and agrees with the findings contained in this report and a Management Action Plan has been developed to address the recommendations (**see Annex C**).

1.0 INTRODUCTION

As outlined in its 2009-2010 Report on Plans and Priorities, CSC has established five priorities in response to the changing offender profile. One of the identified priorities is the "*safety and security of staff and offenders in our institutions*". An important element in support of this priority is the safeguarding of offender and staff records.

CSC employs 15,400 employees, of which approximately 85% work in either an institution or in the community. Furthermore, CSC is responsible for approximately 13,500 incarcerated offenders.[2] The Service is responsible for the proper creation, management and safeguarding of offender and staff records. Offender records contain personal and other sensitive information on an offender's background, criminal history, health, and case management while in the custody of CSC. Staff records may also contain potentially sensitive personal information. It is therefore important for CSC to ensure that there is appropriate safeguarding of records to reduce safety and security risks to staff and offenders in institutions.

The Information Management Division, under the Corporate Services Sector[3], is responsible for the management of corporate information at National Headquarters and creates information management standards, policies and programs in accordance with all Federal Government policies. In addition, this division is also responsible for management of the Offender Records. The Information Management Division also provides functional direction to both regions and institutions with regards to physical offender files. However, the Division has minimal involvement with the management of physical staff records as this falls under the responsibility of the Human Resource Management Sector.

The Regional Headquarters are responsible for the safeguarding of the victims physical files, however they are not responsible for safeguarding any other physical files regarding offenders. Staff members at the Regional Headquarters (RHQ) are also responsible for the safeguarding of any physical staff files which are being maintained at RHQ. While the structure of the various RHQs varies, most regions have a designated administration section to whom the institutions can ask for advice and procedures regarding the appropriate methods to safeguard physical offender and staff records.

Within the institutions, the Chief of Administration reporting to the Assistant Warden Management Services is responsible for the management of all physical corporate and offender records. Responsibility for physical staff records varies between institutions, however, at many institutions it is the Labour Relations Advisors whom are responsible for the safeguarding of the physical staff files.

[2] Reports on Plans and Priorities – 2009-10

[3] Effective April 2010, the Information Management Services Branch will report directly to the Senior Deputy Commissioner.

Several pieces of government policy and legislation relate to the safeguarding of information. The legislation and policies that are relevant to the safeguarding of both offender and staff records include:

- *Privacy Act*
- *Access to Information Act*
- *Government Security Policy*[4]
- *Policy on Privacy Protection (Treasury Board)*

The following are some of the legislation, policies and procedures specifically relating to the safeguarding of offender records:

- *Corrections and Conditional Release Act (CCRA)*
- Commissioner's Directive 568 (*Management of Security Information*)
- Commissioner's Directive 568-6 (*Creation, Control and Handling of Preventive Security Files*)
- Commissioner's Directive 568-9 (*Management of Human Sources*)
- Commissioner's Directive 701 (*Information Sharing*)
- *Records Management Operations Procedure Manual (CSC)*
- *Guide to Information Security* (CSC)
- *Offender Records System User's Guide* (CSC)

At this time, no national procedures or manuals exist for dealing specifically with the safeguarding of staff records. This is further discussed in Section 4.1.1.

1.1 Legislation and Government Policies

The *CCRA* addresses many elements relating to the creation, maintenance and sharing of information collected regarding offenders. The *CCRA* requires that information regarding an offender's personal history be obtained as it is relevant to administering a sentence *(s. 23(1))* including information relating to the court proceedings and victim impact statements. Given the nature of this information, it stipulates that completeness and accuracy are essential *(s.24(1))*. In the case where an offender is of the opinion that information pertaining to him/her is factually incorrect and requires amending, the *CCRA* specifies that a request should be submitted to the Service by the offender and a notation should be made if warranted *(s. 24(2))*.

The Privacy Act (s.8) states that information sharing can take place between a government department and a third party if certain parameters are met. The *CCRA* (s. 25) provides specific guidance for disclosure of information by CSC to third parties including the Royal Canadian Mounted Police (RCMP), the National Parole Board (NPB), the Canada Revenue Agency (CRA) and victims. If an offender wishes to access information about him/herself, Section 2 of the CCRA holds that a written request for information should be submitted; offenders are entitled to access any

[4] Subsequent to the approval of the audit report by the Audit Committee, the Government Security Policy has been changed to Policy on Government Security.

information that would normally be disclosed under the *Privacy Act* or *Access to Information Act*. Information that may jeopardize the safety of an individual, the security of an institution or a lawful investigation is not shared with offenders *(s. 27).*

The *Privacy Act*, Government Security Policy (GSP) and *Access to Information Act*, serve as a basis for the protection of information within governmental bodies. This includes outlining roles and responsibilities at a governmental level as well as at a departmental level. The GSP delegates responsibility to various bodies, such as the RCMP who must determine the requirements for physical security. In addition, the GSP requires that departments appoint a Departmental Security Officer to establish and direct a security program which includes training and awareness and sharing of information among other responsibilities. In addition, the GSP requires that there be a staff member who is familiar with the security requirements of safeguarding documents. The *Privacy Act* further stipulates the requirements and conditions of information that can be collected and the uses thereof. Other elements described include the classification and filing of protected information, security clearance, restriction of access, tracking of disclosure and the retention and disposal of information. The GSP outlines cases of reportable breaches and requires that departments develop a process for completing investigations of suspected breaches.

1.2 Key Processes and Procedures

Various Commissioner's Directives (CDs) and manuals serve to emphasize and reiterate the safeguarding responsibilities as set out in the *Privacy Act* and *GSP*. For example both CD 701 Information Sharing and the Guide to Information Security Manual provide direction relating to the importance of 'need to know.' Need to know is defined in CD 701 as "a need to acquire information for purposes that are currently related to the staff member's duties" (s. 17). 'Need to know' is paramount; security clearance is not sufficient evidence that an individual requires access to particular information. This is taken into consideration not only when information sharing takes place between CSC employees, but also with third parties such as the NPB or the RCMP.

Given the sensitive nature of some information, it is necessary to track access and movement of records in order to safeguard records against inappropriate access and loss or breach of information. Accordingly, the Offender Records System User's Guide describes the process by which physical offender files are tracked: the Master Control Index Card (MCIC) records the permanent location of a file, a charge-out card is used and placed on the shelf in lieu of the specific file when the file has been borrowed and the file jacket is used to track who has accessed a specific file.

Offender related information is divided into 13 file banks including case management, health care, preventive security and victims among others. The majority of this information is stored at the offender's institution, with the exception of the victim file which is stored at the Regional Headquarters and the mental health treatment centre file which remains at the treatment centre. According to the departmental information classification plan, employee personnel records include file banks related to pay and benefits, career management, compensation and leave.

Offender information held at the institution is transferred along with the offender when needed. Other offender information created at the institution, such as records relating to the administration of offender complaints and grievances and claims against the Crown, remain at the institution in which they were created.

The key definitions regarding protected information are as follows:

- **Protected Information:** information related to other than the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or *Privacy Act*, and the compromise of which would reasonably be expected to cause injury to a non-national interest.
- **Protected A:** applies to information with low sensitivity that, if compromised, may cause minimal injury, generally of a personal or commercial nature. For example: disclosure of an exact salary figure, one's age, religion or ethnic origin.
- **Protected B:** applies to particularly sensitive information that, if compromised, could reasonably be expected to cause injury, outside the national interest, to a person or organization, or when it contains information otherwise considered particularly sensitive. For example: performance evaluations, psychological or psychiatric reports, personal financial data, all Offender Management System information, or information that may result in a loss of reputation or damage to a business's competitive advantage.
- **Protected C:** applies to the very limited amount of extremely sensitive information that, if compromised, could reasonably be expected to cause extremely grave injury outside the national interest. For example: information about police informants, Crown witnesses or offenders who have committed crimes that place them at risk from the general prison population, if the offence were known; certain elements of contingency plans, etc.

Information regarding staff is designated as either Protected A or B, while the majority of information regarding offenders is designated as *Protected B*. The exception to this occurs with the Preventive Security and the Victim files which are designated as *Protected C*.

As offenders are being transferred to various institutions, their offender file banks are to be transferred as well. In a routine transfer, all files are to accompany the escorting officer during the transfer. In the case of a transfer that is deemed as an Emergency Transfer, as a minimum, the Health Care, Psychology and Preventive Security files are to accompany an offender, with the remaining files being transferred the next day. When files are being transported they must meet the Information Security Requirements regarding security markings, wrapping, transportation method and storage. Additional tracking takes place for institutional transfers compared to files used within an institution; a Records Transmittal Note and Receipt (CSC 0827) accompanies all files being transmitted. This form specifies all files being sent and upon receipt is consulted, confirmed and returned to the original sending institution within 72 hours.

1.3 CSC Internal Audit of Privacy

In 2006, the CSC Internal Audit Branch conducted an Audit of Privacy[5], which focused on four major areas, one being the management framework in place with respect to privacy. Concerns were noted about the management framework needing improvements specifically regarding roles and responsibilities with respect to privacy being unclear as well as clarification to the process to deal with a breach of privacy.

Following the Audit of Privacy, several recommendations were made of which three have some relevance to our current audit. One recommendation called for a comprehensive accountability framework to be developed for privacy activities, while another one recommended the review of the reporting and monitoring system to clearly define the reporting requirements and ensure a consolidation and analysis of the information. The third recommendation called for the development and implementation of a national strategic communication and training plan with respect to the protection of personal information amongst other things.

Since this audit, changes have been made to the accountability framework for Privacy and direction on roles and responsibilities with respect to both the management of the Access to Information process and a formal process has been documented to report respective breaches. The Policy Sector has also introduced a Privacy Committee, comprised of members from various sectors, to share information and lessons learned in order to minimize the risk of further breaches occurring.

Additional work is currently underway to develop a communication and training plan for the protection of personal information. Awareness sessions provided by ATIP are expected to be completed by the end of fiscal year 2009-2010.

[5] http://www.csc-scc.gc.ca/text/pa/adt-prvcy-378-1-204/audit_privacy2006-eng.shtml

2.0 AUDIT OBJECTIVES AND SCOPE

2.1 Audit Objectives

The audit objectives were:

- To provide reasonable assurance that the management framework in place supports the effective safeguarding of physical offender and staff records; and
- To provide reasonable assurance that CSC is in compliance with the various legal and policy requirements related to the safeguarding of physical offender and staff records.

2.2 Audit scope

The audit was national in scope and included site visits to institutions in each region and to select Regional Headquarters. Interviews, observations and file reviews were conducted at each site to assess both the existing management framework with regards to records management and the compliance with relevant CSC and TBS policies and legislation such as the *Privacy Act.*

The audit did not examine the adherence to appropriate retention and disposition schedules. Safeguarding of electronic files was also not included in this audit as this area was recently examined in the Audit of Logical Access Controls[6]. As well, the audit did not examine offender records held within the community, however, if warranted, this topic may be covered in future audit work at the community level.

3.0 AUDIT APPROACH AND METHODOLOGY

In reviewing the management framework, the audit team reviewed the policies and procedures in place relating to safeguarding of physical offender and staff records along with the roles and responsibilities and any training provided to the various individuals responsible to safeguard physical records. The audit team also examined any processes in place relating to monitoring and reporting.

In assessing compliance with relevant policies and legislation, the audit team examined how information was being classified and filed and how access to the information was being controlled. Controls around records in transit and the retention and disposition of records were also examined as part of the audit.

Various methods were used to gather evidence including:

- **Interviews:** 103 interviews were conducted with a sample of Assistant Wardens Management Services, Chiefs of Administration Services, Custodians of sub-

[6] http://www.csc-scc.gc.ca/text/pa/adt-lac-378-1-240/adt-lac-378-1-240-eng.pdf

registries, Parole Officers, HR Officers, Subject Matter Experts in Security, Human Resources and Information Management and Records Clerks.

- **Review of Documentation:** Relevant documentation such as policies, procedure manuals, training material, and monitoring and reporting information was reviewed and analyzed.
- **Site Visits:** In order to select a sample of institutions, the Corporate Reporting System was used to generate a collection of data reports, including institutional offender population and offender transfer volumes between institutions. Some physical records are stored at Regional Headquarters, including some institutional staff files and the Victim's File. The following factors were considered in site selection:
    - Security level (i.e. Minimum, Medium, Maximum, Multi);
    - Institutional function (i.e. Reception centre, Women's Institution, Healing Lodge, Treatment Centre);
    - Transfer Volume (i.e. transfers in, transfers out, Penitentiary Placements, interregional transfers);
    - Number of breaches reported to ATIP;
    - Institution Population; and
    - Location of files.
- **File Review:** A randomly selected sample of offender and staff files was reviewed at each site visited to determine compliance with legislation and policy and to assess the effectiveness of the elements of the management framework. The sample included:
    - 986 offender files (covering the 13 different file banks including a review of the Master Control Index Cards / offender file inventory cards);
    - 138 transfer-in files (offenders transferred to the institution visited);
    - 147 transfer-out files (offenders transferred from the institution visited); and
    - 350 staff files consisting of compensation, leave, training and performance review files.
- **Observation (walk arounds):** Observation checklists were completed at each site to determine compliance with policies, such as availability of appropriate disposal methods and storage of files and the audit team visited each area of the institution that maintained physical offender or staff records.
- **Analytical Review:** Analytical reviews were performed throughout the audit in order to identify trends, including best practices.

In addition, debriefings were held with senior management at each institution and in the regions. In addition, the Assistant Commissioner, Corporate Services, the Assistant Commissioner Correctional Operations and Programs and the Assistant Commissioner Human Resource Management were debriefed on the overall findings of the audit. Draft reports were provided to senior management for comments and preparation of the Management Action Plan.

4.0 AUDIT FINDINGS AND RECOMMENDATIONS

4.1 Management Framework

We assessed the extent to which an appropriate management framework is in place to support the proper safeguarding of physical offender and staff records. This included a review of directives and guidelines, training material, organizational structure, roles and responsibilities, and reporting and monitoring mechanisms.

4.1.1 Policies and Procedures

We expected to find that CSC policies, procedures, guides and manuals are clear, sufficient to support the proper safeguarding of records and consistent with relevant legislation and government policies.

Offender records

CSC's current policies and procedures for safeguarding of offender records are consistent with relevant legislation and government policies. Procedures and user's manuals are comprehensive and generally well understood by staff.

The Security Branch within the Correctional Operations and Programs Sector has issued a "Guide to Information Security" to adapt the Government of Canada Security policy to the CSC environment. There are also specific provisions in various CDs for the management, conservation and storage of preventive security, medical, psychiatric and victim files. These policies are owned by the subject matter experts (Security, Health Care, Correctional Operations and Programs) responsible for the monitoring and functional coordination of these policies.

Information Management has created a comprehensive manual called "Offender Records System User's Guide" (98 pages) to provide detailed guidance about what files to create to manage offender records, what forms to keep in what file, etc. This guide has been reviewed as recently as June 2009.

Staff records

With respect to records management and safeguarding of physical staff records, little national guidance exists.

Based on the guidance and direction in existence for offender records, we would have expected a similar approach to be in place for the management of physical staff records. This would include the Human Resource Management Sector, in collaboration with the Information Management Division providing guidance to staff on the appropriate management of the physical staff records. However we found that minimal policies and guidance are provided to the Regions and to the institutions for the management of physical staff records.

The only guidance issued by NHQ can be found in the CSC information classification plan and focuses on the filing code for four files (General file, Attendance and Leave, Performance Review and Training). In the absence of national guidance, one region (Québec) has developed a record management manual for staff records called “The Procedures Manual – Employee Records” that could serve as a good tool to share across CSC. The other regions informed us that they are waiting to receive guidance from NHQ before issuing instructions to staff on how to manage and safeguard employee files.

4.1.2 Roles and Responsibilities

We expected to find that roles and responsibilities assigned to CSC functional authorities in NHQ are clear, well defined, documented and understood by staff. We also expected that the roles and responsibilities of employees directly involved in the safeguarding of physical offender and staff records are defined, documented and understood.

Offender records

Corporate responsibilities for safeguarding of physical offenders records among NHQ Sectors are well defined and understood, but are not clearly documented.

The audit team did not find any policy or framework document that would clearly describe the various sectors’ responsibilities with respect to the safeguarding of physical offender records. When browsing through CSC Sectors’ InfoNet sites, there are references on several of them about their role in this process.

The Information Management Division of the Corporate Services Sector states that it is responsible for all aspects related to managing corporate information, including offender records management. Access to Information and Privacy, within the Policy Sector, refers to their role of ensuring that appropriate safeguards are respected regarding the protection of personal information. The Security Branch, within the Correctional Operations and Programs Sector, is the Office of Primary Interest (OPI) for the Commissioner’s Directive 568 on the management of security information.

By reading the information posted on the various InfoNet sites, it is clear that each of the above mentioned sectors has a role to play in the protection and the safeguarding of offender information. Through the review of this information and interviews with various sectors, the audit team identified the key sectors at NHQ who have responsibilities with regards to safeguarding of physical offenders records. The Departmental Security Branch is responsible for creating the policies regarding safeguarding, including determining classification of information and specific safeguards to be used with regards to files. It is then the responsibility of the Information Management Branch to write manuals and provide direction to the regions and institutions in order to ensure that the safeguarding of physical offender records complies with the policies issued by the Departmental Security Branch. The Information Management Division also has a functional responsibility over the physical offender records; however there is no formal reporting relationship between the Information Management Division and staff managing the physical offender records in either institutions or Regional Headquarters.

Based on the interviews held with the Information Management Services Branch and the Security Branch, it appears that the two branches understand their roles with regards to the safeguarding of physical offender records. However, the roles and responsibilities are not clearly documented. As a result, there is not a clear understanding to users in the regions of whom to contact with questions and issues related to the safeguarding of offender records.

Staff records

Corporate responsibilities for safeguarding of staff records are neither defined nor documented.

The Human Resource Management Sector’s InfoNet site mentions that it serves as a focal point for the resolution of administrative and human resource activities and for providing interpretations of policies, directives and guidelines. There is no direct reference to staff records on the Information Management Division’s InfoNet site.

As mentioned under Section 4.1.1, we expected to find a process in place for the management of physical staff records similar to the one that exists for the management of physical offender records. Based on the interviews we conducted, the responsibilities at the corporate level are not clear. Recent discussions with the Human Resources Management and Corporate Services Sectors confirmed that the roles and responsibilities should be better defined for both Sectors.

Staff involved in the safeguarding of staff and offender records understand their roles and responsibilities.

95% of staff interviewed stated that they understand their roles and responsibilities as they relate to safeguarding of information. We were able to collect job descriptions for many of the positions that we interviewed. Through analysis of this documentation, we determined that not all of those involved in the process have their record management/safeguarding responsibilities explicitly stated in their job descriptions. Those that did not contain a statement to this effect were typically job descriptions for people having custody of certain offender files in the sub-registries (extended charge-out) in positions such as parole officers, correctional officers, nurses, etc. However, although the roles and responsibilities are not explicitly stated in all of these job descriptions, staff members are generally aware of their responsibilities, as discussed above.

4.1.3 Training

We expected to find that training and awareness relating to the safeguarding of physical offender and staff records is sufficient, available and provided to staff where required in a timely manner.

Formal training related to the safeguarding of staff and offender records for CSC personnel is limited and while some training material exist, it is not being updated regularly.

Interviews with Chiefs of Administration, Offender Record Clerks working in the central registry, and staff managing files within sub registry indicated that there is limited training provided to these employees. We noted that 50% of the staff interviewed in the above positions have received formal training related specifically to file/records management and 56% of these interviewees felt that they, or their staff, would benefit from additional training.

It was noted during interviews that general training regarding levels of protection and general safeguarding requirements were discussed briefly in various courses such as the New Employee Orientation Program or the Parole Officer Orientation Course. It was stated that while the coverage of these topics is fairly brief, for the majority of staff whose role is not centered on managing a registry, the training provided was adequate.

The training provided to staff responsible for safeguarding of physical records varies between regions as some regions offer formal training sessions and some offer nothing. In one region, the Regional Chief of Administration from time to time provides formal training sessions to institutional records clerks and separate training to sub registry record holders. The audit also noted that some institutions have started the practice of having the Security Intelligence Officer provide training regarding information management, to staff members during institutional orientation sessions.

Training tools are available to all CSC staff via the Information Management Division's intranet site. Training modules have been developed to educate staff regarding the legislation, policies and procedures related to Information Management in CSC. They are intended for records management staff and staff designated with record keeping responsibilities in our organization. One of the main modules is General Records Management (November 2003) which contains information on file/records management in general including descriptions of information classification levels (classified and designated), relevant legislation and policies, general requirements on filing, management and disposition of records, etc. Another key module is the Offender Information Management (June 2005) which provides information about the offender records system, records classification (13 files), offender file management, file routing and the management of inactive records. Unfortunately, not only are these tools not known by the staff working in the institutions, but they appear to be outdated, based on the date of the last revision.

The lack of resources was cited as the main reason why formal training for records staff was not provided on a regular basis. Any training provided to these staff members is usually peer to peer when there is a change in the incumbent of the position. Although on the job training can be very thorough as it is done one-on-one, it also has the potential to perpetuate incorrect practices. Furthermore, the lack of formal training leads to inconsistencies of the methods in place to safeguard records in the various institutions. The limited training that is provided to records staff regarding records management can explain to some extent some of the areas of non-compliance that were identified as part of the audit (refer to section 4.2).

Based on the results of the audit, there would be benefits in training staff on topics such as the 'need to know' principle, classification of documents, and procedures to apply when accessing an offender's file. For example, as discussed in Section 4.2.3, there is a misunderstanding regarding the requirement to sign or annotate the front cover of files whenever they are accessed and not just when the files are removed from a central registry.

With regards to the management of physical staff records, the lack of national direction and procedures makes it even more difficult to deliver consistent training. The risk associated with staff receiving limited training may increase the number of security and/or privacy breaches.

4.1.4 Monitoring & Reporting

We expected to find a process established to report performance at national, regional and institutional levels regarding the safeguarding of physical offender and staff records, including monitoring compliance and assessing continuous improvement.

Reporting mechanisms are in place to report on and to manage breaches; however, limited reviews and information sharing are undertaken to improve CSC practices.

There is no formal requirement related to the monitoring and reporting of the performance in managing and safeguarding physical offender and staff records. The safeguarding of physical records is not an area that is given attention at higher levels unless problems, such as breaches, occur.

In 2009, the ATIP Division created a document called "Guidelines on Privacy Breaches" which streamlines the reporting process regarding a privacy breach. When privacy breaches occur, there is a formal process to report on them through the Institutional Head, through to Regional and ultimately National Headquarters. The process may involve the Security Branch, the Access to Information and Privacy Branch and Information Management Services Branch. Once a breach has been reported, an assessment of the severity will occur. For breaches that are deemed to be either moderate or high sensitivity, notification will be sent to the individual whose information has been breached. In many cases, corrective measures will be implemented, and notification of their completion will be provided to the reporting authority. Some of the common types of breaches that are reported include providing offender information to the incorrect offender, losing an offender file and inappropriate access by staff to offender records for which there is no need to know. The different types of breaches that relate to the safeguarding of physical records which were observed as part of the audit will be described in Section 4.2. While there are well documented procedures to report an incident, no other corporate monitoring and reporting has been implemented.

During our visits, we noted that a few institutions are performing a yearly quality review of the physical offender files under the custody of both their central registry and sub-registries. This review includes a reconciliation of the inventory of existing files (Master Control Index Cards or equivalent) with the files in the filing cabinet as well as a review of the major control/quality points of the files such as documents in the right file, documents well secured in the jacket, proper maintenance of files, etc. These reviews are beneficial in monitoring compliance, in ensuring that all files are accounted for and in identifying opportunities for improvement. However, these reviews are not consistently done across institutions and the results are not shared.

Good Practice
At some institutions, central registry staff would complete a quality review in the sub registries and selected staff from the sub registries would perform a review in the central registry to ensure independence

With respect to staff files, we are not aware of any system of control for existing staff files nor have we been made aware of any performance monitoring or quality assurance process.

CONCLUSION:

Key elements of the management framework are in place to support the safeguarding of physical offender records. CSC policies and procedures are consistent with relevant legislation and with government policies. Procedures and user guides are comprehensive and generally well understood by staff. Some training tools exist and mechanisms are in place to report and manage privacy breaches.

Nonetheless, our audit showed that attention is required in the following areas:

- There is a need for direction, guidance and clarification of corporate roles and responsibilities with respect to the management and safeguarding of physical staff records;
- Roles and responsibilities with respect to the management of physical offender and staff records should be fully and clearly documented;
- Training should be enhanced; and
- Monitoring and reporting is mainly focused on privacy breaches and could be improved.

RECOMMENDATION 1

The Assistant Commissioner, Corporate Services in collaboration with the Assistant Commissioner, Human Resource Management and the Assistant Commissioner, Correctional Operations and Programs should strengthen the management framework in the following areas:

- Clarify and document corporate roles and responsibilities for the safeguarding of offender and staff records;
- Provide guidance and direction on the requirements for the safeguarding of staff records;
- Improve training tools and provide additional training to staff where needed; and
- Enhance monitoring and reporting processes.

4.2 COMPLIANCE WITH LEGAL AND POLICY REQUIREMENTS

We assessed the extent to which CSC is in compliance with the various legal and policy requirements relating to the safeguarding of physical offender and staff records. This included interviews, file reviews and observational walk-arounds to determine what takes place within the institutions with regards to maintaining, transferring and disposing of records.

4.2.1 Classifying and Filing Records

We expected to find that physical offender and staff records were being appropriately classified and filed.

Records are not always being classified as Protected A, B or C when the information is sensitive.

In 56% of the offender files reviewed, issues were raised with certain documents not being classified. While most forms within the offender files are pre-classified as Protected B, certain forms such as the Officer Statement and Observation Reports (OSOR) require the author to choose the appropriate security levels for the documents, something that is not always done. The audit team also noted that many printed e-mails and documentation created by third parties (police reports etc.) that are filed in the offender records are not being classified.

During the various interviews, it was noted that staff at the institution understand the various levels of protection; however most agreed that they do not always think about identifying the protected level on the various documents.

Information is generally filed in the appropriate individual's file.

In 98% of offender files reviewed, the information regarding an offender was stored in the appropriate offender's file. The result for staff files was equally high. The few instances where information was misfiled can be attributed to human error and does not appear to be a significant systemic issue.

4.2.2 Maintaining Official Files

We expected to find that information on both offenders and staff is placed only in official records and that no shadow files are kept.

Official offender files are well maintained and in accordance with procedures while official staff files are less well maintained.

The audit team noted no major concerns with regards to the state of the offender files reviewed. For the most part, the audit team found that records were permanently affixed to the file folder, and the appropriate file jacket was being used.

Some concerns were raised regarding how closed volumes of records were being dealt with. In 8% of files reviewed, closed volumes were not clearly marked as such, increasing the risks that individuals may be reviewing a previous volume of information and not being aware that there is more recent information available.

As discussed in Section 4.1.1, there is no national direction relating specifically to staff records, and concerns were noted regarding the current state of some of these records. The overall maintenance of staff records varied significantly between institutions but the audit team noted many instances of information, particularly in the leave and training files, not being permanently affixed to the folder. This leads to the possibility that sensitive staff information can more easily be lost.

Shadow files and temporary files are being used by some institutions.

Shadow files are copies of official records that are being stored separate from the official file. The Offender Records System User's Guide states that shadow files should not be used. The audit team raised concerns regarding the use of these shadow files during the site visit.

For example, all of the institutions visited within two regions maintain a duplicate copy of the employee compensation file within the institution as the original file is held at RHQ.

Another example of a shadow file involves Parole Officers maintaining an unofficial file on offenders assigned to their case load. These files contain specific reports that the Parole Officers access on a regular basis.

The risks involving shadow files include a greater chance that some information may inadvertently be filed only in the shadow file thus increasing the risk that the official file may be incomplete. Furthermore, additional files in existence increase the risk of information breaches occurring where individuals may have access to information that they should not have.

Concerns were also raised regarding temporary files which were found to exist in various institutions. The Offender Records System User's Guide states that temporary files are to be controlled and maintained similarly to official files; however this is not being done. The temporary files are usually plain manila folders, with information not permanently affixed to the file.

For example, the audit team noted three institutions that maintain temporary files for offenders who are in segregation. In these cases, the Segregation unit maintains a temporary file, while the official Discipline and Dissociation (D&D) file remains in the central registry. From time to time the information in the temporary file would be amalgamated with the official D&D file, however the central registry did not have any record of the temporary file being in existence.

The use of temporary files creates the risk that information can easily be lost or otherwise misfiled. Furthermore, the central registry is not made aware of the existence of these temporary files. As such, there is no accurate record that additional information is being maintained elsewhere leading to the possibility that an individual who needs to review a file may be unaware that they are not reviewing all of the available information on the subject.

Institutional staff does not always clearly identify which personal information documents have been given to an offender.

In accordance with the *CCRA*, offenders are to be provided copies of certain information acquired by the Service. To obtain information, offenders are to make a request through the formal access to information process. Offenders can also request information from various institutional staff members, and if it is a routine report they are requesting, copies of this information will usually be provided at that time. For example, it is common for an offender to ask his or her Parole Officer for a Case Management report that has previously been shared. Most Parole Officers interviewed stated that they regularly provide offenders additional copies of reports; however if they have any concerns about providing it, they will instruct the offender to request the information through the formal ATIP process.

While CSC is required to allow offenders to have access to their personal information, there is no mechanism in place at most institutions to identify what documents have been given to them. Should a breach occur as a result of an offender having in his/her possession personal information about another offender, it is almost impossible for CSC to determine if such breach results from CSC not having safeguarded the information properly or if the information found was the unprotected property of an offender. Some institutions would annotate any documents provided to an offender by using an "Offender Copy" stamp.

GOOD PRACTICE

Some institutions would annotate any documents provided to an offender by using an "Offender Copy" stamp

Our analysis of the Situation Reports (SITREP) report shows that since April 1, 2007 there have been a total of 27 reported occurrences of offenders being found to be in possession of information regarding a different offender. Without a mechanism in place to determine if the information retrieved was a copy that had been shared with an offender, it is very difficult to determine in how many of the occurrences was the institution responsible for the inappropriate sharing of the information and where there is a need to take corrective measures.

4.2.3 Access to Records

We expected to find that processes existed to ensure access to records is restricted to a need to know basis and is appropriately logged.

File jackets are not always being signed or annotated when files are accessed.

Several different sources, including the *Privacy Act*, state the requirement to be able to identify who has accessed an individual's personal information and for what purpose. The Offender Records System User's Guide states that in order to satisfy this requirement records staff must ensure the front of the jacket is completed, stating who has accessed the file and why. Through observations and interviews within the various registries, the audit team noted several instances of non-compliance with access not being recorded on the file jacket.

During interviews with records staff it was noted that some individuals mistakenly believed that signing the front of the file jacket was only required when removing the file from the registry.

Many registry staff visited stated that while they attempt to ensure the reasonableness of the request to review a specific file, they do not ensure that the file jacket is being properly signed or annotated. The lack of awareness regarding the importance of the appropriate signing of file jackets causes the institutions to be in non-compliance with the *Privacy Act.*

The "Need to know" principle is well applied with regards to access by offenders of personal information about other offenders; however it is much less emphasized with regards to access by staff of offender personal information only when a need to know is confirmed.

During the observations and interviews at the various institutions, the audit team was able to determine that the importance of safeguarding protected information when offenders have access to an area with private information is well understood. Interviewees stated that they take precautions to ensure that offenders are not in a position where they can obtain or see protected personal information on other offenders or staff. For instance, Parole Officers stated that whenever an offender is in their office, they place information face-down or otherwise out of the offender's sight.

While it was apparent that staff understands the requirement of the "need to know" principle with regards to offenders, it was also clear that for the most part, the "need to know" requirement regarding offender information by staff was not as tightly controlled. Staff is not always questioned when accessing, or requesting access to, offender information in the central and sub registries. For example it was noted in many interviews that although most institutions have a list of each Parole Officer's caseload, it is rarely referred to.

Significant concerns were noted at one institution where the central records office was self-service; it allowed any staff member access to any offender file without question or monitoring. Thus it was difficult for this institution to ensure that the need to know requirement was being followed. During the site visit to this institution, the Warden was informed of this issue and corrective action has since been taken.

One exception to the issues surrounding the "need to know" is Preventive Security Offices. At all Preventive Security offices visited, Security Intelligence Officers (SIO) were found to be very cautious when providing access to the files. Due to the sensitive nature of Preventive Security files, SIOs only provide access to a specific file if the individual has a valid reason. At some institutions, the SIO required that any staff member requesting access to a file must first document the request, including his/her name, the offender's name and the reason for accessing the file. This information was retained in an easily accessible listing which provided a clear history of files accessed.

Maintaining access on a need to know basis for staff is further complicated by the existence of joint offices and shared printers and photocopiers. For example, at one institution, the electronic equipment was being shared with Health Care, Psychology V&C and Parole Officers. At any time, an individual may print a document and someone, who does not have a need to know, could easily access this information.

Furthermore, according to policy, staff offices in locked areas with access controls are considered to be a security zone and in such a zone, Protected B information can be maintained on open bay shelving. While it is true that offenders do not have access to these offices, other staff can easily access information for which they do not have a clear need to know.

Overall, access to files by offenders is restricted but the need to know requirement by staff is generally not being followed and inappropriate access to information by staff may occur within the institutions.

On the other hand, the "need to know" for staff files is better controlled. Based on the interviews with HR staff members, it was apparent that access to the files is limited. Should anyone ask to review an HR file, the HR staff verifies the individual's need to know prior to providing access.

4.2.4 Records in Transit

We expected that there would be a system in place to identify and track the movement of files.

Logs of access are maintained for files charged out to the users; however, follow-up does not always exist to ensure files are returned in a timely manner.

At many of the registries visited, it was noted that no formal follow-up process was in place to ensure files are returned in a timely fashion. Approximately half of the Central Registry Records Clerks did not have a method for follow up on the timely return of the files. Through observations and interviews it was noted that registries in the institutions had processes in place to track which files had been signed out, however there was a lack of consistency in the methods between institutions and between registries within an institution. For example, some institutions use charge out cards and place them on the shelf in lieu of the actual files, while others maintain log books stating when the specific file was removed and by whom. Processes and timelines as to how long a file can be charged out varied by institutions. Some institutions allowed individuals to charge out files for as long as needed while others would require all files to be returned at the end of the day unless prior approval is obtained. Even within the same institution, methods used for tracking charged out files varied between the various registries.

Lack of appropriate follow up procedures to ensure files are returned in a timely manner increases the risk that files may go missing and unreported. Furthermore, the possibility that new information is not added to a file in a timely manner increases when a file is charged out for a lengthy period of time.

In several institutions, there is a gap in the accountability for the files while they are in transit between institutions.

While the institutions are using controls when files are in transit, such as the Document Receipt and Transmittal forms, there is a lack of accountability as to who is responsible for the files during the transfer. The Administration staff in the sending institution is responsible for boxing and wrapping all of the files, however the files leave their control once the CSC driver or escorting officer takes the files. During interviews, records staff in various regions stated that escorting officers do not take ownership of the files.

While some institutions have developed a good practice to have the escorting officers or CSC drivers sign for the number of boxes they take responsibility for, there is currently no such requirement in the policy. At the majority of institutions visited, there was no process in place to assign accountability for the files. During interviews, the audit team was informed of occurrences of files not arriving with the offender and difficulties encountered in tracking the files. Based on our review of the SITREPs, there have been two reported instances of offender files being lost while in transit between institutions since April 2007. Having the CSC drivers or escorting officers sign for what they have received will increase the accountability and the control over what is being transferred.

Boxes of files awaiting transfer were being held in areas of the institution where individuals who do not have a need to know could access the information.

Concerns were noted at various institutions with the way boxes of files were being handled. For example, at one institution, all files awaiting transfer to the Regional Depot were being stored under desks in the administration section. These boxes included all files on offenders that have passed their warrant expiry date including the Protected C Preventive Security file. During interviews, administration staff at this institution stated that although they understand the importance of proper safeguarding of records, the lack of space in the records room forces them to look for alternatives.

At another institution, offender files were being held at the main security office of the building for several days, awaiting the transfer of the offender. Again at this institution, interviews with administration staff suggested that the importance of safeguarding of records was recognized but operational requirements left staff with no other options. At this institution, we were told that it was difficult to know exactly when the offenders may be transferred and therefore, the files needed to be accessible at any time.

Lack of control over the boxes once they leave the records office increases the possibility that the files may be inappropriately accessed or misplaced. While it is unlikely that offenders will have the opportunity to access these boxed files, it is quite possible for other staff members to do so. Shortage of space and operational requirements sometimes force institutions to disregard some rules regarding the safeguarding of information.

Files are being wrapped appropriately while in transit between institutions.

At the institutions visited no issues were noted regarding the wrapping of documents. Policy states that Protected information should be in a double sealed envelope with the inner envelope marked with the appropriate Protected level and must clearly state "to be opened by addressee only**”.** All individuals that we interviewed regarding this process understood how to appropriately wrap and transmit the files.

4.2.5 Storage of Records

We expected to find methods in place to ensure that records are being appropriately stored according to their sensitivity.

Physical staff records are being stored in accordance with Protected B requirements.

The audit team found in both institutions and at Regional Headquarters, physical staff records were being stored in accordance with policy. In all cases, we noted that staff records were being stored in a locked area with controlled access. Furthermore, we also noted that information was locked in filing cabinets when the files were not being used.

Preventive Security Files are not always stored in accordance with Protected C requirements.

At seven out of the 17 institutions visited, issues were raised with the safeguarding of the Preventive Security files. At four of the institutions, the audit team noted that the cabinets being used for the storage of the files did not satisfy the RCMP Equipment Standards for storing Protected C information.

At three other institutions, closed volumes of the Preventive Security files were being stored on the shelves in the Central Records Office. The storage of records on shelves within an office is only appropriate for the storage of information designated up to Protected B.

Files being used outside of the institution are not always appropriately safeguarded.

While teleworking frequently occurs at many institutions, it is uncommon for staff to bring physical files outside of the institution. At the majority of the institutions visited the audit team was told that staff working from home would regularly access the required reports electronically through the Offender Management System (OMS). The exception to this occurred at the various assessment units visited. Parole officers and other staff at these institutions do telework on a regular basis. However, since at the point of intake, very little information exists on the various CSC systems, teleworking staff need to have the official offender file to complete their work. While staff are allowed to do telework, the policy states that a threat risk assessment (TRA) must be completed on the work environment where the files will be stored. There was no evidence that this was occurring at the institutions visited. Furthermore, while some of these institutions have acquired appropriate locking briefcases to carry these files, none of the employees we interviewed claimed to use the briefcases. It should be noted that there have been 5 reported occurrences to the SITREP regarding the loss of files while they were outside of the institution.

4.2.6 Disposal of Records

We expected to find that records were being disposed of appropriately according to their sensitivity.

Protected information of both offenders and staff is not always being disposed of in an appropriate manner.

Through interviews it was determined that most individuals understand the importance of properly disposing of sensitive information. Various disposal methods are available in institutions including shredding bins, shredders or maintaining individual shredding boxes under their desks until the information can be disposed. However, at some institutions it was noted that information is not always being disposed appropriately.

Many of the institutions visited have shredding bins located in various areas of the institution. These shredding bins, used to dispose of personal offender and staff information up to Protected B, are locked and can only be opened by staff in the administration section and by the shredding company. These containers are emptied and the content shredded based on a pre-determined schedule, normally once or twice per month. The audit team was told that the administration staff could empty the bins between shredding dates and store the shredding elsewhere within the institution; however it is unclear how frequently this occurs.

During the walk-arounds, the audit team noted several bins at various institutions that were over-flowing and where information could easily be removed through the opening at the top. Not only does this increase the risk that staff could access information that they do not have a need to know for, but the bins are sometimes located in areas of the institution where offenders roam, increasing the risk that they could easily obtain some sensitive information.

Another example of inappropriate disposal was noted during the observation in the Segregation unit at one institution. In this case, Correctional Officers working in this unit did not have easy access to a shredder or a shredding bin. The Officers stated that while they understand the importance of shredding it was simply not convenient to take the shredding to an appropriate shredder, and as such would regularly place this information into their garbage for disposal.

From the institutions that were not appropriately disposing the information, various reasons were provided to explain why this was not being done. The audit team heard that the location and number of shredders and shredding bins was not always adequate in order to ensure convenience and ease of shredding. The lack of shredding bins was also given as a reason why the bins were sometimes overflowing. Furthermore, based on our review of the SITREP, there have been at least six reported cases regarding sensitive information being found in the garbage since 2007.

CONCLUSION:

While we found many practices that comply with the various safeguarding requirements related to the classification, filing, maintenance, access, movement, storage and disposal, we also noted areas of non-compliance as follows:

- Some documentation in files, primarily observation reports, printed e-mails and documents created by third parties, are not being marked as Protected when necessary;
- There are several instances where staff files were not well maintained, including several documents not being affixed to the folder;
- Shadow and temporary files are being used within many institutions and offices;
- Documents given to offenders by CSC are not always properly identified;

- File jackets are not always signed or annotated when individuals access an offender file;
- The “need to know” principle is not always well applied, especially with regards to access by staff to offender personal information;
- There are gaps in the safeguarding of the offender records in transit within and/or between institutions;
- Files, including in some cases Preventive Security records, are not always stored appropriately based on the sensitivity and protection level of the documentation; and
- Protected information is not always being disposed of appropriately.

The enhancements recommended in Section 4.1 with respect to training on the requirements related to the safeguarding of physical offender and staff records should assist CSC in improving overall compliance. In the interim, it would also be beneficial to remind staff of the safeguarding requirements for both offenders and staff records. Further, additional measures are needed to strengthen the controls for offender files in transit.

RECOMMENDATION 2

The Assistant Commissioner Corporate Services, in collaboration with the Assistant Commissioner Correctional Operations and Programs, the Assistant Commissioner Human Resources Management and the Regional Deputy Commissioners, should ensure that all staff comply with the policies, including the areas of non-compliance identified in this report such as:

- Marking documents that are not already protected when filing them;
- Signing or annotating the file jackets whenever the files are accessed;
- Properly identifying information given to offenders by CSC;

- Discouraging the use of shadow and temporary files and ensuring that the official files are complete;
- Reinforcing the requirement to apply the “need to know” principle when accessing files; and
- Reviewing and enhancing key controls around staff accountability and safeguarding requirements for offender files transferred between institutions, the storage of files based on the sensitivity and protection level of records, the use of physical records outside of institutions and the disposal of protected information.

ANNEX A

AUDIT OBJECTIVES AND CRITERIA

OBJECTIVES	CRITERIA
1. To provide reasonable assurance that the management framework in place supports the effective safeguarding of physical offender and staff records.	1.1 *Policies and Procedures* - CSC Policies, guides and manuals are sufficient to support the proper safeguarding of physical offender and staff records and are consistent with existing legislation and government policies. 1.2 *Roles & Responsibilities* – Roles and responsibilities related to the safeguarding of physical offender and staff records are clearly defined, understood and documented. 1.3 *Training* – Training as it relates to safeguarding physical offender and staff records is clear, sufficient, available and is provided where required in a timely manner. 1.4 *Monitoring & Reporting* – There is a process established to report performance at national, regional and institutional levels, regarding the safeguarding of physical offender and staff records. This includes monitoring compliance and assessing continuous improvement.
2. To provide reasonable assurance that CSC is in compliance with the various legal and policy requirements related to the safeguarding of physical offender and staff records.	2.1 *Collection and Use* – Physical offender and staff records are appropriately classified and filed. 2.2 *Collection and Use* – Information on physical offender or staff records is only placed in official records and no shadow files are kept.

OBJECTIVES	CRITERIA
	2.3 *Collection and Use* – Access to physical offender and staff records is restricted to a need to know basis and is appropriately logged. 2.4 *Records in Transit* – There is a system in place to identify and track the movement of physical offender records.* 2.5 *Storage of Records* – Physical offender and staff records are appropriately stored according to their sensitivity 2.6 *Disposal of Records*– Physical offender and staff records are appropriately disposed of according to their sensitivity.

* Pertains to offender records only

ANNEX B

Location of Site Visits

Atlantic Region
Regional Headquarters
Springhill Institution – Medium Security
Westmorland Institution – Minimum Security
Shepody Healing Centre / Dorchester Penitentiary – Multi-level Security

Ontario Region
Regional Headquarters
Regional Treatment Centre – Multi-level Security
Millhaven Institution (Assessment Unit) – Maximum Security
Frontenac Institution – Minimum Security

Pacific Region
Mountain Institution – Medium Security
Fraser Valley Institution – Multi-level Security
Pacific Institution (Regional Reception and Assessment Centre) – Multi-level Security

Prairie Region
Rockwood Institution – Minimum Security
Stony Edmonton Institution – Medium Security
Edmonton Institution for Women – Multi-level Security
Edmonton Institution – Maximum Security
Pê Sâkâstêw Centre – Minimum Security

Quebec Region
Regional Headquarters
Archambault Institution – Medium Security
Special Handling Unit / Regional Reception Centre– Maximum Security
Federal Training Centre – Minimum Security

ANNEX C

AUDIT OF SAFEGUARDING OF PHYSICAL OFFENDER AND STAFF RECORDS MANAGEMENT ACTION PLAN

RECOMMENDATION	ACTION SUMMARY	OPI	PLANNED COMPLETION DATE
Recommendation 1: The Assistant Commissioner, Corporate Services in collaboration with the Assistant Commissioner, Human Resource Management and the Assistant Commissioner, Correctional Operations and Programs should strengthen the management framework in the following areas:	Establish a Committee with representation from the Information Management Division of the Corporate Services Sector, the Departmental Security Branch of the Correctional Operations and Programs Sector and Human Resource Management Sector.	Information Management Division, Corporate Services Sector, NHQ.	February 2010
• Clarify and document corporate roles and responsibilities for the safeguarding of offender and staff records;	a. Clarify corporate roles and responsibilities of NHQ Sectors for the safeguarding of offender and staff records.	Information Management Division, Corporate Services Sector, NHQ / Departmental Security Division, Correctional Operations and Programs Sector, NHQ / Human Resources Sector, NHQ	May 2010
	b. Ensure roles and responsibilities for safeguarding offender and staff records are formally documented in policy or other framework documents.		December 2010

RECOMMENDATION	ACTION SUMMARY	OPI	PLANNED COMPLETION DATE
• Provide guidance and direction on the requirements for the safeguarding of staff records;	Develop Information Management User Awareness program for CSC Employees:	Information Management Division, Corporate Services Sector, NHQ / Human Resources Sector, NHQ	March 2011
	Review and or update CSC policies and CD's as required, to ensure that specific provisions for the management, security, conservation and storage of staff records is consistent with relevant legislation and government polices.	Information Management Division, Corporate Services Sector, NHQ / Departmental Security Division, Correctional Operations and Programs Sector, NHQ / Human Resources Sector, NHQ	March 2011
• Improve training tools and provide additional training to staff where needed; and	Develop formal training program for Information/Records Management staff:		
	a. Update records management General and Offender Records Training Modules	Information Management Division, Corporate Services Sector, NHQ	May 2010

Recommendation	Action Summary	OPI	Planned Completion Date
	b. Develop records management training module specific to Staff Records	Information Management Division, Corporate Services Sector, NHQ / Human Resources Sector, NHQ	December 2010
	c. Develop Security of Information Management Module for use in conjunction with Information Management Training Modules	Departmental Security Division, Correctional Operations and Programs Sector, NHQ	May 2010
	d. Schedule and deliver training	Information Management Division, Corporate Services, NHQ/Regions	March 2011-December 2011
	Develop Information Management User Awareness program for CSC Employees:		
	a. Develop Module specific to information management roles and responsibilities in relation to offender and staff records.	Information Management Division, Corporate Services Sector, NHQ / Human Resources Sector, NHQ	August 2010

Recommendation	Action Summary	OPI	Planned Completion Date
	b. Develop Module specific to Security of Information for use in conjunction with the Information Management User Awareness Module (i.e. assigning security classifications to records, storage, packaging and transmission)	Departmental Security Division, Correctional Operations and Programs Sector, NHQ	August 2010
	c. Schedule and deliver training	Information Management Division, Corporate Services, NHQ/Regions	March 2011- December 2011
• Enhance monitoring and reporting processes.	Develop a monitoring and quality assurance process for offender and staff files.	Information Management Division, Corporate Services, NHQ	March 2011
Recommendation 2: The Assistant Commissioner Corporate Services, in collaboration with the Assistant Commissioner Correctional Operations and Programs, the Assistant Commissioner Human Resources Management and the Regional Deputy Commissioners, should ensure that all staff comply with the policies including the areas of non-compliance identified in this report such as:	Review and improve controls for the disposal of protected information particularly where shredders are used as the disposal method by institutional staff and communicate to staff.	Information Management Division, Corporate Services Sector, NHQ / Departmental Security Division, Correctional Operations and Programs Sector, NHQ / Regional Deputy Commissioners	April 2010

RECOMMENDATION	ACTION SUMMARY	OPI	PLANNED COMPLETION DATE
• Marking documents that are not already protected when filing them; • Signing or annotating the file jackets whenever the files are accessed; • Properly identifying information given to offenders by CSC; • Discouraging the use of shadow and temporary files and ensuring that the official files are complete; • Reinforcing the requirement to apply the "need to know" principle when accessing files; • Reviewing and enhancing key controls around staff accountability and safeguarding requirements for offender files transferred between institutions, the storage of files based on the sensitivity and protection level of records, the use of physical records outside of institutions and the disposal of protected information.	Develop national guidelines to improve the accountability of escort officers/staff for offender files while in transit between institutions and document in policy/CD.		June 2010
	Develop a national mechanism for identifying which personal information has been given to offenders by institutional staff and document in policy such as CD or guideline.		June 2010
	Issue a series of communiqués reminding staff of the need to comply with the various requirements including: a. Requirement for marking documents, signing and annotating file jackets b. Ensure access to personal information on offenders and staff is to be based on the principle of "need to know" and appropriate level of security c. Ensure boxes of files stored in areas outside of the Main Records Office are protected from unauthorized access d. Ensure that staff records and Preventive Security Files are stored in accordance with security guidelines for protected information e. Ensure that a threat risk assessment of the work environment has been completed and is current where staff are using offender files at home locations as part of tele-work arrangements to complete their work		June 2010
	f. Ensure that offender and staff records are filed on official files		