Correctional Service Canada | Service correctionnel Canada

SAFETY, RESPECT AND DIGNITY FOR ALL

LA SÉCURITÉ, LA DIGNITÉ ET LE RESPECT POUR TOUS

Audit of Privacy of Offender Information

Internal Audit Sector

May 15, 2014

Canada

This page is left blank to allow for double sided printing.

Table of Contents

Executive Summary

Background

The Audit of Privacy of Offender Information was conducted as part of Correctional Service Canada's (CSC) Internal Audit Sector's 2012-2015 Risk-Based Audit Plan. The audit linked to several corporate priorities for CSC including "safety and security for staff and offenders in our institutions and in the community" and "efficient and effective management practices that reflect values-based leadership." Additionally, the Audit of Privacy of Offender Information linked to CSC's corporate risk that "CSC will not be able to maintain required levels of operational safety and security[1]."

A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information. A privacy breach may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders. Privacy breaches within CSC are self-reported and are classified by level of risk based on the private information which was compromised.

The Audit of Privacy of Offender Information was national in scope and focused on the overall privacy of offender information and the prevention and reporting of privacy breaches of this information.

The audit objectives were to:

- provide reasonable assurance that the management framework in place ensures the privacy of offender information and is in accordance with various acts and legislation; and
- provide reasonable assurance that CSC is ensuring that the privacy of offender information is maintained as required by the applicable legislation, acts and departmental frameworks.

Conclusion

Overall, the audit found that the management framework needs to be strengthened in order to ensure that the privacy of offender information is maintained. Guidelines on Privacy Breaches have been created, shared and are generally considered clear.

[1] *Corporate Risk Profile at a Glance, December 2012*.

However, there are areas where additional work can be done to improve the management framework. These include:

- the roles and responsibilities for those responsible for reporting and tracking privacy breaches at the local level need to be better defined;
- management must ensure that all privacy breaches are being reported;
- training and/or awareness sessions should be provided to institutional staff;
- staff awareness of what constitutes a privacy breach and how to report a breach once discovered is lacking; and
- National Headquarters (NHQ) should accurately track, monitor and examine privacy breach trends by region and institution.

Moreover, CSC has processes in place to report privacy breaches, and for the privacy breaches that were known by NHQ, privacy risk assessments were completed. In addition, the hard drives of all CSC laptops are encrypted. Furthermore, a basic knowledge of the need-to-know principle is possessed by staff. However, CSC could improve compliance with the relevant guidelines relating to the management of privacy of offender information. These include:

- ensuring that the need-to-know principle is consistently interpreted and applied across CSC;
- mechanisms should be used to identify offender report copies;
- institutions should ensure that appropriate methods to dispose of offender information are used;
- non-encrypted and untracked portable media devices should not be used throughout the institutions; and
- institutions should ensure that personal offender information is collected from printers and photocopiers in a timely manner.

Management Response

- *A/ACP agrees with the overall audit findings and recommendations as presented in the audit report.*
- *A/ACP has prepared a detailed Management Action Plan to address the issues raised in the audit report.*
- *The Management Action Plan will be implemented by July 31, 2014. Some actions will be conducted on an ongoing basis (such as ATIP training and awareness sessions).*

Statement of Conformance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The opinion is applicable only to the area examined.

The audit conforms to the Internal Auditing Standards for Government of Canada, as supported by the results of the quality assurance and improvement program. The evidence gathered was sufficient to provide senior management with proof of the opinion derived from the internal audit.

_____ Date: _____

Sylvie Soucy, CIA
Chief Audit Executive

1.0 Introduction

The *Audit of Privacy of Offender Information* was conducted as part of Correctional Service Canada's (CSC) Internal Audit Sector's *2012-2015 Risk-Based Audit Plan*. The audit linked to several corporate priorities for CSC including "safety and security for staff and offenders in our institutions and in the community" and "efficient and effective management practices that reflect values-based leadership." Additionally, the Audit of Privacy of Offender Information linked to CSC's corporate risk that "CSC will not be able to maintain required levels of operational safety and security."

A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information. A privacy breach may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders. Types of privacy breaches include, but are not limited to; theft or loss of records, miscommunication (i.e. email/mail sent to the wrong address), unauthorized access of personal information and unauthorized disclosure (i.e. inappropriate display of personal information).

Privacy breaches within CSC are self-reported. Privacy breaches are classified by level of risk based on the private information which was compromised. It is ultimately up to the office of primary interest (OPI) to determine the severity of risk. The six year breakdown for the number of CSC internally reported breaches per year is presented below.

Number of CSC Breaches Reported Internally Per Year

2006/07	2007/08	2008/09	2009/10	2010/11	2011/12
84	75	83	157	111	205

Legislation and Policy Framework

The *Privacy Act* gives Canadians the right to know how their personal information is collected, used, disclosed, retained and disposed of; and gives them the right of access to that information. Within CSC, personal information holdings include information about employees, offenders and members of the public (i.e. victims). Personal information under the control of the government shall not, without consent, be disclosed[2]; however the *Privacy Act* specifies the circumstances where personal information, held in trust, may be disclosed. For example, CSC staff has access to such information for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose[3] (day-to-day job duties) and CSC may release personal information to the general public when the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure[4].

[2] The Privacy Act. Section 8.
[3] The Privacy Act. Section 8(2)(a).
[4] The Privacy Act. Section 8(2)(m)(i).

The *Access to Information Act* provides individuals with a right of access to information in records under the control of government institutions. These access rights are not absolute and are subject to limited and specific exceptions.

The Privacy Commissioner of Canada, whose mission is to protect and promote the privacy rights of individuals, submits to Parliament its Annual Report on the *Privacy Act*. This report includes topics such as key accomplishments, challenges and initiatives for the years ahead. In addition, the report also contains statistics of the number of breaches for the 10 federal departments with the most reported breaches. According to the Privacy Commissioner's 2011-2012 Annual Report to Parliament, CSC reported a total of 54 privacy complaints. For the tenth straight year CSC accounts for the largest number of privacy complaints received by the Privacy Commissioner.

Guidelines on Privacy Breaches have been prepared by the Access to Information and Privacy (ATIP) Division at National Headquarters (NHQ) (henceforth referred to as the ATIP Division) to describe the process to deal with privacy breaches, including how they are to be reported and how to conduct privacy risk assessments (PRAs) at the operational level where the impact and the circumstances of the breaches are best known.

Public servants are expected to abide by the *Value and Ethics Code for the Public Service*. This code forms part of the conditions of employment in the Public Service of Canada. All public servants are responsible for ensuring that they comply with this code and demonstrate the values of the public sector in their actions and behaviour. One such value is stewardship, where public servants shall "acquire, preserve and share knowledge and information as appropriate." If a public servant does not abide by these values and expectations, they may be subject to administrative or disciplinary measures up to and including termination of employment.

Treasury Board (TB) *Policy on Government Security* ensures that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management. Government security is the assurance that information, assets and services are protected against compromise. The policy requires all deputy heads to establish a security program that has a governance structure with clear accountabilities, has defined objectives that are aligned with departmental and government-wide policies, priorities and plans.

Previous Audits

In 2006, the Internal Audit Sector completed an *Audit of Privacy*. This audit found that the management framework for privacy addressed certain roles and responsibilities and provided direction on specific aspects of privacy within CSC. However, the audit identified a concern regarding a general lack of understanding amongst staff of what constitutes a real or potential privacy breach. As well, the audit found that while some breaches were being investigated, the process was not consistently applied and clear direction was lacking at the national level. A total of eight recommendations were made as part of this audit. To date, management has indicated that all eight recommendations have been completed. Three of the eight recommendations from this audit pertained to the disclosure of health information and consent forms. Similar issues

were raised during the *Audit of Regional Treatment Centre and the Regional Psychiatric Centre* in fiscal year 2010-2011 and have yet to be fully implemented.

The *2008 Audit of Logical Access Controls* found that monitoring had been enabled and activities performed to monitor unauthorized access to high profile offender cases in Offender Management System (OMS) and security incidents which, have been defined as OMS security incidents, were monitored and followed up on a regular basis.

Finally, in 2010 the Internal Audit Sector completed the *Audit of Safeguarding of Offender and Staff Records*. This audit indicated that key elements of a management framework were in place to support the safeguarding of offender records. The audit also found that CSC policies and user guidelines were consistent with relevant legislation and with government policies and mechanisms were in place to report and manage privacy breaches. However, the audit also found that training should be enhanced and that the need-to-know principle was not always being applied, specifically with regards to access by staff to offender personal information. Two recommendations were made as part of this audit and management has implemented the measures developed in their action plan for both recommendations.

Privacy Breach Reporting Process

When a privacy breach is discovered, the person who uncovers it takes immediate action, where possible, to reduce the severity of the breach and must report the breach immediately to his/her manager. The OPI for the specific breach is identified at the working level. The Guidelines on Privacy Breaches state that an OPI is assigned for every breach but the specific person identified as the OPI can vary for each breach. The ATIP Division may be consulted at any time during the process.

The OPI carries out an initial assessment of the circumstances, and if necessary, takes additional steps to reduce the severity of the breach and advises the ATIP Division via email. Next, the OPI completes a PRA to ascertain the level of risk and forwards the PRA to the reporting authority (the ATIP Division). Privacy breaches are rated higher in terms of severity if they are deemed to have an impact on an individual's safety or sense of privacy, thus potentially affecting public and/or employee confidence in CSC's ability to manage its personal information holdings.

The OPI determines if notification of the individual whose information has been breached is required. The notification informs the individual of the incident and of his/her right to file a complaint to the Office of the Privacy Commissioner of Canada (OPC). Treasury Board's Guidelines for Privacy Breaches strongly recommends that notification be made when the breach: 1) involves sensitive personal data such as financial or medical information or the Social Insurance Number; 2) can result in identity theft or other related fraud; 3) can otherwise cause harm or embarrassment which would have detrimental effects on the individual's career, reputation, financial position, safety, health or well-being.

The OPI determines whether a fact finding investigation is needed, and if so, initiates one. The determination is based on the need to gather additional facts in order to recommend measures to avoid a similar incident and/or to assess the risk or impact caused to the individual. Normally, a fact finding investigation is required for a moderate or high severity breach (unless the facts are very clear when the PRA is completed).

When a fact finding investigation is conducted, the report is submitted to the ATIP Division. Any corrective measures taken or that will be taken are identified in the report.

Finally, the ATIP Division is required to notify the OPC of all moderate and high risk breaches.

CSC Privacy Management Framework

Following the *2006 Audit of Privacy*, a Privacy Management Framework (PMF) was created within CSC. The PMF ensures that privacy is a core consideration in the management of personal information so that management practices and service delivery reflect the spirit and requirements of the *Privacy Act*. The PMF is a productive instrument in reducing corporate privacy risk. As part of PMF implementation, CSC's Guidelines on Privacy Breaches were created to replace the previously used privacy breach protocols.

The *Audit of Privacy* also indicated that a lack of coordinated management of privacy issues existed amongst sectors at NHQ. As a result, a Privacy Committee was established to oversee PMF implementation. The Privacy Committee, who meets quarterly, is mandated to perform the following functions:

- provide a senior level review of privacy issues and challenges to the management of personal information at the operational level;
- facilitate culture change at the operational level so that regions, local management and staff are fully engaged in mitigating any privacy risk to the management of personal information;
- review particular risk issues escalated for its consideration and monitor the implementation of the TB Privacy Impact Assessment (PIA) Policy; and
- analyze the impact on CSC of privacy issues raised by the privacy community, especially the OPC.

The Privacy Committee is chaired by the Assistant Commissioner, Policy and members include the Director of the ATIP Division, senior officials from various Sectors, along with regional and institutional representatives.

2.0 Audit Objectives and Scope

2.1 Audit Objectives

The audit objectives were to:

- provide reasonable assurance that the management framework in place ensures the privacy of offender information and is in accordance with various acts and legislation; and
- provide reasonable assurance that CSC is ensuring that the privacy of offender information is maintained as required by the applicable legislation, acts and departmental frameworks.

The audit criteria for this engagement, which assisted in meeting the audit objectives, originated from the Committee of Sponsoring Organizations (COSO) for the first objective and from TB and CSC's Guidelines on Privacy Breaches for the second objective. Specific criteria related to each of the objectives are included in ***Annex A***.

2.2 Audit Scope

The *Audit of Privacy of Offender Information* was national in scope and focused on the overall privacy of offender information and the prevention and reporting of privacy breaches of this information. A sampling of institutions from all five regions, ensuring coverage of each security level and each type, was visited as part of the audit. A listing of the institutions visited can be obtained in ***Annex B***.

The audit assessed whether controls were in place to ensure that breaches to offender information were being reported and that management had processes in place to ensure that the likelihood of breaches occurring and reoccurring were minimized. The audit examined CSC directives and frameworks surrounding privacy to ensure that they were consistent with relevant acts and legislation and examined compliance with the concepts within the *Privacy Act* including the principle of need-to-know. The audit also looked at whether methods were in place to protect private offender information. Moreover, the audit also assessed the awareness of CSC employees relating to privacy breaches of offender information along with their roles and responsibilities in this area.

The scope of this audit was limited to offender information and did not examine the privacy of either staff information or of offender information held in the community. The audit also did not examine the determination for the classification of offender information (i.e. protection levels) or the process surrounding access to information. The timeframes surrounding reporting of breaches were not reviewed since the accuracy of these timelines could not be verified.

3.0 Audit Approach and Methodology

The audit team reviewed legislation, policies and procedures in place related to the offender privacy process, the roles and responsibilities of staff in the institutions, training and awareness, the reporting of privacy breaches and the monitoring and reporting occurring at these sites.

The audit team also assessed compliance with key legislation, policies and guidelines and with key internal controls related to the offender privacy process. Compliance was tested through observations, analytical review, documentation review and interviews with staff at the institutions to both assess the management framework and to ensure that the privacy of offender information was being upheld.

Annex C lists and describes in further details the techniques used to gather evidence to complete this audit.

4.0 Audit Findings and Recommendations

4.1 Management Framework for the Privacy of Offender Information

We assessed the extent to which a management framework was in place to support the effective management of offender privacy. This included a review of legislation, policies and guidelines, roles and responsibilities, training and awareness and monitoring and reporting mechanisms.

4.1.1 Policy and Procedures

We expected to find that guidelines and bulletins existed to support the privacy of offender information and that they were in line with relevant Acts, Legislation and Government of Canada policies. We also expected to find that they had been communicated to employees.

Guidelines to support the privacy of offender information were in place and had been communicated to staff.

In 2010, the ATIP Division issued *Guidelines on Privacy Breaches*. These guidelines described the process to deal with privacy breaches, including how they are to be reported and how to conduct the PRAs to determine the impact and circumstances surrounding the individual breach. These guidelines were updated in 2013 to conform to recommendations made by the OPC. Some of the changes to the framework include the requirement of notifying the OPC of all medium and high level privacy breaches, including copies of all documents which were breached along with the completed PRA, the notification letter and any other relevant supporting documentation. If a breach is of a very low risk level (i.e. an email sent to the wrong CSC employee containing personal information of a non-sensitive nature), it is at the discretion of the OPI to determine if a PRA and breach notification are necessary.

During interviews, the audit team found that all wardens, assistant wardens, management services and chiefs of administration services interviewed were aware of the *Guidelines on Privacy Breaches* and 92% (33/36) of them stated having read through the guidelines. In addition, 78% (29/37) of interviewees stated that they found the guidelines to be clear and raised no concerns with the requirements. Of the interviewees who raised concerns, issues included difficulty in determining who at the institution is ultimately responsible for determining whether a fact finding investigation is necessary, difficulty in determining the level of the breach and even difficulty in determining if the privacy concern raised was actually a breach.

The *Guidelines on Privacy Breaches* were updated during the conduct phase of this audit. The audit team did not assess or differentiate between the 2010 and 2013 guidelines when testing management and staff awareness of said document.

CSC's* Guidelines on Privacy Breaches *were in line with the Privacy Act and Government of Canada Policy.

The audit team compared both the 2010 and updated 2013 *CSC Guidelines on Privacy Breaches* to the *TB Guidelines for Privacy Breaches* and to relevant sections of the *Privacy Act*. Overall, no discrepancies or contradictions were noted between the documents.

4.1.2 Roles and Responsibilities

We expected to find that roles and responsibilities related to governance and to ensuring the privacy of offender information were clearly defined, understood and documented.

Although the responsibility for managing privacy breaches is clearly defined in the job description for the chief of administration services, the guidelines did not formally assign any roles.

In reviewing the national generic job description for the chief of administration services position, the audit team noted that this individual is to act as the designated institutional lead for all matters related to privacy and access to information, provide advice to management, ensure institutional staff compliance with relevant legislation and develop appropriate corrective measures. The job description also says that this individual will implement and recommend any necessary corrective action to management. When reviewing CSC's 2013 *Guidelines on Privacy Breaches*, it was noted that it does not specifically assign responsibility to a specific individual, rather allowing the sites to customize as appropriate.

Wardens, assistant wardens, management services, chiefs of administration services, and security intelligence officers play a significant role in the reporting and monitoring of privacy concerns at the institutions. During interviews with these individuals, the audit team found that while interviewees understood their role in the event that a breach was found, there was little consistency between sites on the process to report and follow-up on privacy breaches of offender information. At nine of the 15 sites visited, all breaches were reported to and managed by the assistant warden, management services, the chief of administration services or a specific individual working for these individuals. At these sites, this person would be the main point of contact for all privacy concerns at the site, would coordinate any required fact finding investigation, would complete the PRA and report the breaches to the required individuals as appropriate.

At the remaining sites, the process was much less consistent, and much less clearly defined. For example, at some sites, we found that breaches were to be reported to the Security Intelligence Officer. In other sites, the audit team found that the staff were notifying Regional Headquarters (RHQ) and/or NHQ privacy groups directly when they had concerns that a privacy breach may have occurred. For the majority of these sites where the chief of administration services was not the predominant point of contact for the management of the privacy breaches, it was even less clear who would be responsible for approving and ultimately managing any corrective measures which would be included in the PRA to minimize the likelihood of this breach recurring.

The lack of specifically defined roles in the CSC *Guidelines on Privacy Breaches* detailing who is responsible for the management of privacy breaches, allows for increased confusion and the likelihood that staff are not reporting all breaches or are not managing them consistently across the country. The reporting of privacy breaches is further discussed in Section 4.1.4.

4.1.3 Training and Awareness

We expected to find that training related to maintaining the privacy of offender information has been developed and delivered to all CSC employees and that staff understood the various principles as they related to the privacy of offender information.

Minimal training had been delivered to staff at the institutions.

Training is offered to employees so that they can acquire the knowledge and skill requirements pertaining to their roles and responsibilities. As part of the New Employee Orientation Program (NEOP), Parole Officer Induction Training and CORE training for correctional officers, new employees are given a very high level awareness session regarding privacy including need-to-know, protection level of documents, and safeguarding of electronic information. Of staff interviewed, 52% (65/124) said they had received some training as part of one of these orientation programs. However, only 37% (24/65) of these people have received additional training related to privacy.

During interviews with the ATIP Division and with the Regional ATIP Liaison Officers, the audit team found that while it is desirable to provide training sessions pertaining to privacy, these interviewees stated that due to time and other budgetary constraints, limited training has been offered to the institutions.

Staff understood the concept of privacy of information but did not always understand what constitutes a privacy breach.

During observations and interviews at the various institutions visited, the audit team was able to determine the importance of safeguarding protected information, when offenders have access to an area with private information, is well understood by staff. Interviewees stated that they take precautions to ensure that offenders are not in a position where they can obtain or view any personal information belonging to someone else. For example, staff repeatedly stated that, whenever an inmate cleaner is in their office, they place information face-down or otherwise out of the offender's sight, turn off their computer monitors and never leave the offender unattended in an office. However, as further discussed in Section 4.2.2, the safeguarding and management of offender information varies when it is another staff member who wishes to access offender records. This lack of protection of offender information when dealing with other staff members is in violation of the need-to-know principle.

Staff interviewed felt the privacy topic was not a difficult one and does not require constant training. That said, as privacy breaches continue to occur, the audit team noted examples where

e-mails were sent to staff reminding them of their obligations with respect to the care and protection of personal and protected information. As well, some institutions visited were planning to conduct awareness sessions at venues such as staff assemblies to help share the message about the importance of privacy.

The audit team found evidence, through both interviews and observations, that some breaches were occurring but not being reported. For example, the audit team observed an inmate returning a report to the correctional officer window stating that it was given to him by error. This, however, was not reported as a privacy breach as the Correctional Officer did not believe it was necessary. The audit team heard from institutional management and Regional ATIP Liaison Officers that a large reason why privacy breaches were not being reported was due to a lack of awareness by institutional staff on what constitutes a privacy breach. This lack of awareness was also raised as an issue in the 2006 *Audit of Privacy*.

4.1.4 Reporting of Privacy Breaches

We expected to find that formalized processes exist and are being followed to ensure the reporting of privacy breaches of offender information.

While a framework existed to report privacy breaches, inconsistencies were found between sites for how this framework was being applied.

The 2013 *Guidelines on Privacy Breaches* describe the process to deal with privacy breaches, including how they are to be reported and how to conduct the PRAs. As previously discussed in Section 4.1.1, the guidelines have been shared extensively throughout CSC and most wardens, assistant wardens, management services and chiefs of administration services are well aware of the guidelines along with the requirements to ensure privacy breaches are reported as required. That said, as discussed in Section 4.1.2, the roles and responsibilities related to privacy issues and breaches at the institutions are not always clearly defined.

The guidelines state that the person who uncovers the breach is to report it directly to their manager who will identify the OPI. The guidelines also state that the OPI will carry out an initial assessment of the circumstances, advise the ATIP Division of the breach and complete a fact finding investigation and the PRA. During interviews at the institutions, the audit team noted that at many of the sites visited, individuals were unclear how to report a suspected or known privacy breach or who to speak with to obtain this information. The audit team did note that at sites with a significant number of reported privacy breaches, individuals were well aware of the process to follow and who at the institution would be the main point of contact to discuss concerns with breaches. However, at sites that had reported very few privacy breaches, the audit team found that individuals were unaware of whom to report a privacy breach to, thus increasing the likelihood that many breaches of offender information were going unreported.

The audit team also found that at two sites, it was the security intelligence officers who were responsible for reporting privacy breaches. Concerns were noted by the audit team that when a

privacy breach was reported to this position, they would report the breach through the security breach process, but would not complete the required steps of the *Guidelines on Privacy Breaches*. In this case, the ATIP Division stated that they would still learn of the breach when they reviewed the daily Situation Reports. That said, during discussions with the Security Branch at NHQ, the audit team confirmed that not all privacy breaches of offender information would be included in the Situation Reports. As such, some privacy breaches may be occurring without ever being tracked by the ATIP Division.

Not all breaches were being reported.

The *Guidelines on Privacy Breaches* define a privacy breach as the improper or unauthorized collection, use, disclosure, retention and / or disposal of personal information which results from poor personal information management. During interviews with staff from the ATIP Division, all Regional ATIP Liaison Officers and 59% (10/17) chiefs of administration services and assistant wardens, management services stated that, in their view, not all privacy breaches were being reported. The audit team heard varying reasons behind why not all breaches were reported including; the culture of the institutions, fear of reprimand and an overall lack of awareness by some CSC staff on what actually constitutes a privacy breach.

During audit observation, it was found that privacy breaches are occurring at some sites due to systemic processes, although the staff at the institutions seemed unaware that these caused privacy concerns. These processes were often part of the culture of those institutions. For example, the audit team found offender call lists identifying offender name, partial FPS number and where and when they had an appointment posted throughout two institutions. Concerns were also raised regarding offender count boards in the units at three sites, which were in visible areas to both staff and offenders and which would include offender name, FPS number, and other personal information including incompatible offenders and gang affiliation. These issues were also noted in the 2006 internal *Audit of Privacy*.

During interviews at sites, specifically those with fewer reported breaches, the audit team found that the culture of the institution supported the perception that it was not considered important to report all privacy breaches. As previously noted, the audit team also found a link between poor awareness by staff on what constitutes a privacy breach and the number of breaches which have been reported. The lack of reporting raises concerns that CSC will be unable to stop privacy breaches from reoccurring if they are not being made aware that these breaches are occurring and the reasons behind them. If the breaches are not being reported, CSC will not be able to inform offenders regarding breaches to their personal information, thus becoming non-compliant with the *Privacy Act*. Furthermore, offender safety may be jeopardized if these systemic issues continue.

4.1.5 Monitoring and Reporting

We expected to find that management monitors reported privacy breaches to ensure that reoccurring breaches are minimized and that the fundamental causes are corrected.

The Access to Information and Privacy Division monitored the privacy breaches reported to them to ensure that privacy risk assessments were being completed as required. However, this division was not able to provide accurate statistics for individual sites.

The *Guidelines on Privacy Breaches* require that the OPI dealing with the specific breach must report it to the ATIP Division within two days of the breach being uncovered and must also complete the PRA to determine the level of risk of the privacy breach. The guidelines, which explain the seven types of privacy breaches, require that individuals send an email to a generic account varying by the type of breach. Once this email is sent, the appropriate groups within NHQ are carbon copied to ensure they are made aware. For example, to report the theft or loss of hardcopy records, the individual would send an email to GEN-NHQ Breach/Atteinte Type 1 and this would automatically ensure that the ATIP Division and Departmental Security were made aware of this breach.

Through interviews with staff at both the institutions and NHQ, the audit team confirmed that this process was occurring for breaches where the institutions were reporting. That said, the audit team raised concerns that, while the ATIP Division could accurately track breaches which occurred throughout the service during a specific timeframe, the system was unable to accurately provide reports demonstrating the breaches which occurred at a specific site. As part of the audit, the audit team requested a listing of all breaches reported since 2011 for the 15 sites visited. When this listing was compared to the breaches that the institutions had on file, the audit team realized that an additional 43 cases existed at the site level. In these cases, the sites provided copies of PRAs which had been sent to the ATIP Division but were not on the site specific listings provided.

The audit team raised these concerns with the ATIP Division and it was stated that up until January 2013 information was not being filed by site. This lack of reporting consistency made it difficult for the ATIP Division to provide an accurate picture of trends that occurred at a specific site or in a specific region. The ATIP Division did however confirm that this process has since been changed, and the new process requires that the site where the breach occurred be clearly entered into the system allowing for more accurate tracking and analyses of privacy breaches.

Corrective measures, as identified in the privacy risk assessments, were not actively being followed up on by National Headquarters. However, the audit team confirmed that this issue has since been corrected.

The *Guidelines on Privacy Breaches* state that corrective measures are key to preventing future breaches and must be recorded in the PRA. A copy of supporting completion documents of all corrective measures, including memos and emails, must be provided with the PRA. It is the responsibility of the ATIP Division to follow up to ensure that the corrective measures identified in the PRA have been implemented as required. Corrective action may include providing training and awareness emails or sessions, along with a review of internal procedures or a review of departmental policies. In the event of moderate and high level breaches, corrective action may also include disciplinary reprimand, revocation of security clearance, suspension and/or termination.

The audit team reviewed a random sample of 25 privacy breaches reported since 2011 and was able to find that corrective action was on file in 22 of the breaches reviewed. That said, the audit team found that while the institutions were usually forwarding evidence of corrective action, there was no mechanism in place for the ATIP Division to easily determine which breaches have had their corrective action fully completed and which breaches were still awaiting corrective actions by the institution.

The above deficiency was noted by the ATIP Division early in the conduct phase of this audit. As such, the process has since been strengthened and the ATIP Division is now using their information management system for breaches to its full potential. All communication related to each individual breach is now kept in an organized method within this system, and the ATIP Policy Officers are regularly following up with the institutions to ensure that corrective action for each breach is completed as stated in the PRA. Furthermore, the system now allows the ATIP Division to clearly differentiate between the breaches which are "closed" and those which are "open" and still awaiting evidence of the corrective measures as staff cannot "close" the file until evidence of corrective action has been received and reviewed.

Conclusion

Overall, the audit found that while *Guidelines on Privacy Breaches* have been created, shared and understood by relevant staff, the audit found that the management framework needs to be strengthened in order to ensure that the privacy of offender information is maintained.

The audit identified the following areas for improvement:

- the roles and responsibilities for those responsible for reporting and tracking privacy breaches at the local level need to be better defined;
- management must ensure all privacy breaches are being reported;
- training and/or awareness sessions should be provided to institutional staff;
- staff awareness of what constitutes a privacy breach and how to report a breach once discovered is lacking; and
- National Headquarters should accurately track, monitor and examine privacy breach trends by region and institution.

Recommendation 1[5]

The Assistant Commissioner, Policy, should develop tools to assist local management in addressing privacy related matters, including consistency in the handling of breaches by individual sites. This could include the elaboration of a clear and consistent process on how to identify breaches, to whom at the institution it should be reported and how the breach is to be handled. Moreover, the Assistant Commissioner, Policy, should monitor privacy breach trends to determine root causes of breaches to minimize the risks to CSC.

Local management, overseen by the Regional Deputy Commissioners, should ensure that the privacy management framework and associated tools have been fully implemented at the local level and that mechanisms have been created to improve staff's awareness regarding the importance of safeguarding of sensitive information.

Management Response

A/ACP, ACCOP and RDCs agree with this recommendation.

Actions Include:

- *The Chief, Administrative Services have been identified as the main point of contact for reporting on institutional privacy breaches to NHQ ATIP and all staff will be advised via CSC News at Work. The identification of key positions and persons will ensure a consistent approach for the reporting of breaches within the operational units.*
- *The Privacy Management Framework document will be revised to effectively demonstrate the importance of managing personal information collected and held within CSC.*
- *Training and ATIP awareness sessions will be developed and delivered to enable CSC employees to increase their awareness of the importance of safeguarding personal information and how to report on privacy breaches. Sessions will be delivered as part of NEOP training, in addition to training delivered by Regional ATIP Liaisons to regional staff.*
- *ATIP will produce a quarterly report which will identify common privacy breaches across CSC and the corrective measures implemented to prevent similar breaches. This report will also be used as a tool to remind staff of the importance of protecting personal information.*
- *For a list of all actions associated with this recommendation, please refer to the Management Action Plan. Full implementation for Recommendation 1 by July 31, 2014, when the first Quarterly reporting will be finalised.*

4.2 Application of Privacy Breach Guidelines

We assessed the extent to which CSC was in compliance with the relevant policy guidelines relating to the management of privacy of offender information. This was done primarily through interviews and on-site observations.

[5] Recommendation requires management's attention, oversight and monitoring.

4.2.1 Analysis of Incident

We expected to find that institutions were completing privacy risk assessments and were providing and implementing corrective actions where needed following a privacy breach of offender information.

Privacy risk assessments are completed for all reported breaches, although not all privacy breaches are being reported.

The *Guidelines on Privacy Breaches* require that the OPI for the privacy breach notify the ATIP Division (and the Regional ATIP Officer if applicable) within two days of the breach being uncovered. The OPI must also complete a PRA to determine the level of risk related to the breach.

During interviews with staff at NHQ, RHQ and at the institutions visited, the audit team confirmed that in most cases the wardens, assistant wardens, management services and chiefs of administration services were aware of the requirement to have PRAs completed for all breaches. In some cases, the audit team found that breaches were reported through security reports and were included as part of the daily Situation Reports. In these cases, the ATIP Division would contact the site directly and ensure that a formal PRA, with corrective action, be completed and forwarded as per the *Guidelines on Privacy Breaches*. During discussions with the Security Branch at NHQ, the audit team confirmed that while many privacy breaches reported via security incidents would be included in the Situation Reports, not all low level risk privacy breaches would be included. This finding confirms that not all privacy breaches were being reported to, or come to the attention of, the ATIP Division.

As previously mentioned, concerns were raised that at some sites, while management was made aware of privacy breaches and that these breaches would be reported as per the *Guidelines on Privacy Breaches*, management believed that not all privacy breaches were in fact being reported. During the course of the audit, many reasons were found why individuals were not always reporting privacy breaches. In many cases, while staff understood the importance of privacy of information, some individuals were actually unaware of what constituted a privacy breach, especially for lower risk events. While all sites were aware of the problems when an offender was found to be in the possession of another offender's information, they did not always formally report breaches where offender mail was inadvertently given to the incorrect offender. The audit team also found that in cases when an offender report was reportedly misfiled in another offenders file, many sites would not consider this to be a privacy breach even though they would be unable to determine who may have viewed this document.

These concerns, along with the earlier concern related to awareness; suggest that more breaches exist than are being reported. In addition, if staff is not informing management of privacy breaches, and breaches are otherwise going unreported, little can be done to ensure these privacy breaches do not continue.

4.2.2 Need to Know

We expected to find that the need-to-know principle was being followed and adhered to in accordance with CSC's privacy framework.

While institutional staff understand the basic concept of need-to-know, it is not being consistently applied to its fullest extent.

Commissioner's Directive (CD) 701 – *Information Sharing* defines need-to-know as any information that is pertinent and necessary to an individual performing his/her duties. While on site, the audit team asked 83 individuals whether they found it difficult to determine if they had a need-to-know. Of those interviewed, 89% (74/83) felt that the principle behind need-to-know was very clear and easy to understand. That said, when they were asked to comment on their interpretation of the need-to-know principle, their answers varied significantly between sites. At many sites, the audit team heard that only basic information is necessary to do any job. For example, at some sites, the audit team heard that unless an offender is on a correctional officer's caseload, they had little reason to review the full criminal history of the offender. In other sites, the audit team found that the need-to-know principle was interpreted that any individual having interaction with a specific offender were allowed to examine the file to the extent they deemed necessary. During interviews with wardens, the audit team noted that their interpretation varied significantly and reflected on their staffs' thoughts on the concept. Of the 13 wardens interviewed, seven stated that need-to-know for staff should be extremely limited, which for correctional officers would be offenders on their caseload or in their living unit. The other six wardens had a much more liberal interpretation of the need-to-know concept and felt that staff should have a right to look up any information on any offender in the institution, the reason being that in their view, safety, security and improved dynamic security was key to the safety of staff and offenders and that security should not be sacrificed to maintain privacy.

While it was apparent that staff understood the requirement of maintaining the privacy of offender information from other offenders, the audit team noted that this was less consistently applied regarding staff accessing offender information. Staff was 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. Concerns were also noted at four institutions where files, including some case management files, were held in self-service locations easily accessible to staff whom may not have a need-to-know. This lack of controls made it difficult for the institutions to ensure that the need-to-know requirement was being followed when staff was reviewing files.

The need-to-know principle with regards to the electronic records of offenders is another area of concern as individuals are aware that they can easily review an offender's file without requesting a hardcopy from the records office. After discussions with the OMS Data Quality and User Support Team at NHQ, the audit team determined that this group has the capability to monitor and track usage, including which offender files a staff member has reviewed and when. That

said, no active monitoring is taking place, and these analysis are only done to respond to special requests by senior management.

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, visits and correspondence and parole offices. At any time, an individual may print a sensitive document and someone, who does not have a need-to-know, could easily access this information.

These issues relating to need-to-know were identified as a concern as part of the 2010 *Audit of Safeguarding of Offender and Staff Records*. The current audit found that many of the concerns previously identified are still problematic at the current time. If the need-to-know principle is not being followed, inappropriate access to offender information may occur.

4.2.3 Safeguarding of Offender Information

We expected to find that controls were in place and being abided by employees to ensure that offender information is upheld and safeguarded throughout the institutions.

Mechanisms developed to identify offender copies of reports are not being used.

In accordance with CD 701 - *Information Sharing*, any information which can be shared directly with the offender should be given immediately to them provided that there are no reasonable grounds to believe that the safety of any individual would be jeopardized by sharing this information. This would include copies of finalized reports in OMS such as Assessments for Decision and Correctional Plan Updates.

As part of the 2010 *Audit on Safeguarding of Offender and Staff Records*, it was noted that while CSC is required to allow offenders access to their personal information, there is no mechanism in place at most institutions to differentiate between the copy given to the offender and the copies being retained by CSC. 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 a breach resulted from CSC not having properly safeguarded the information or if the information found was the unprotected property of an offender. Following the audit, in July 2011, a Case Management bulletin was issued stating that sites must ensure that any information given to offenders by CSC staff is properly identified by use of an "offender copy" stamp.

During the current *Audit on Privacy of Offender Information*, the audit team noted that these concerns were still prevalent, as the majority of staff interviewed at 11 of the 15 sites visited indicated they were still not identifying all reports provided to offenders as an offender copy. The lack of compliance with this requirement to use an offender copy stamp still leaves CSC vulnerable to privacy breaches being reported due to offenders not properly safeguarding their own copies of the information as opposed to CSC not safeguarding it.

Offenders do not always have mechanisms in place to secure their personal information when placed in double bunked cells.

As a result of many legislative changes, CSC has seen its offender population increase. CSC is anticipating that its population will continue to increase over the next few years. To address these increases, CSC has had to increase the number of double bunking cells within the institutions.

During the audit, the team inquired as to how the institution expected offenders to protect their own information when double bunked. While it was noted that offenders have the ability to lock their cell doors, thus having no issues for safeguarding their information when in a single bunk cell, concerns were noted for offenders who were sharing accommodations. At eight of the 13 sites visited where double bunking existed, the sites had processes in place to provide offenders with the ability to safeguard their personal information. At seven of these eight sites, offenders in double bunked cells were provided with lockable boxes and/or cabinets where they could store their personal information away from their cellmate. At the remaining site, management decided that no offender records were to be held in the cells, and all information needed to be stored in the offender's personal effects in the admission and discharge unit. The audit team was told that this decision was made as a means to minimize the muscling of offenders to share their personal information, and criminal histories, with other offenders.

That said, at the remaining five institutions, the audit team found that offenders would be unable to safeguard their personal information in their cell as they did not have any mechanism to safeguard it. During the observations in some double bunked cells, offenders regularly left their personal reports in open areas of their cells where their cellmates could easily access this information. The audit team was told, however, that the lack of locked boxes was a security decision as officers needed to have quick access to all areas of the cell to search for contraband.

Offender documents are, at times, being provided to the incorrect offender typically through offender mail.

Offender mail, including mail from both within and outside the institution, is a significant source of reported privacy breaches each year. Since 2011, a total of 104 privacy breaches have been reported across CSC relating to offenders being provided with mail and reports belonging to another offender.

While on-site, the audit team observed the procedures in place in relation to offender mail and noted that there were many different processes at the various institutions for delivering offender mail. At some sites, correctional officers from visits and correspondence were responsible for delivering the mail directly to offenders whether through individual offender mail boxes or to the cell doors. In other sites, the audit team found that it was unit officers who were delivering the mail to offenders. In most of these cases, officers would display a list of offender names that had mail and the offenders would come directly to the officers to ask for it.

During interviews with representatives from the Inmate Welfare Committees, when asked if offenders in general had any privacy concerns, 10 of the 16 committees interviewed raised concerns with offender mail being provided to the incorrect offender. The risk exists that since the vast majority of reports being provided to an offender is not sealed, it was difficult to know if the offender who incorrectly received the report read it before forwarding it to the correct individual. With offender reports, including Assessments for Decisions and Correctional Plan Updates containing a great deal of personal information, including the offender's criminal profile, a risk exists for the offenders' safety should this private information be shared with another offender.

Some sites still do not have available mechanisms or controls in place to dispose of private offender information.

A concern raised during the 2010 *Audit of Safeguarding of Offender and Staff Records* related to the inappropriate methods used to dispose of personal information. Some of these issues were still found to exist as part of the current audit. Since 2011, a total of 19 breaches have been reported across CSC relating to the inappropriate disposal of offender information.

During the observations made by the audit team, various disposal methods were available in institutions including physical shredders, locked communal shredding bins, or maintaining individual burn boxes under desks until the information could be disposed. The audit team did note concerns with the individual burn boxes being maintained at three sites, as these were found to be very full, and were not being emptied regularly. As these burn boxes were typically under desks, although typically in locked offices, it would be relatively easy for an inmate cleaner or other staff member to have easy access to this private information, thus accessing information for which they may not have a need-to-know.

The audit team raised serious concern at three other sites where, specifically in the living units, no shredders, locked shred boxes or burn boxes were made conveniently available for correctional officers. Correctional officers stated in these units that they would typically tear the information in half and place the report/document in either the garbage or the recycling bin. At one of these three sites, the chair of the Inmate Welfare Committee raised concerns that offenders working in the recycling plant have been known to acquire private information on other offenders through information that staff had placed in the recycling bins.

Inmate Welfare Committees at some sites also raised concern that they do not always have a mechanism to dispose of their own personal information as not all sites will allow them use of the shredder or shredding services. At these sites, in order to dispose of the information, offenders will resort to finding other methods of disposing of it.

In the 2010 *Audit of Safeguarding of Offender and Staff Information*, the audit team raised concern with the use of locked shredding boxes which are shredded by a contract company. During the current audit, while the audit team did not note concerns with these locked shredding boxes, the concerns noted were with personal burn boxes overflowing and the inadequate disposal methods used by some correctional officers. Both disposal methods increase the

likelihood of private information being acquired by other offenders or by staff who do not have a need-to-know for this information.

All sites are using encrypted laptops to safeguard information; however, many sites are still using generic portable media drives.

One significant risk area related to the privacy of offender information involves staff members using electronic media to take offender information outside of the institution. A recent initiative put in place by Information Technology Security requires that all CSC issued laptops must now be encrypted so that, if lost, none of the information stored on the hard drive can be inappropriately accessed. During interviews with 11 chiefs of informatics at the institutions visited, the audit team confirmed that all laptops at these sites are now encrypted. Furthermore, the audit team found that when staff members work from a location other than the institution, the institution encourages staff members to sign out one of the encrypted laptops to work from.

The audit team also verified any controls surrounding the issuance and tracking of USB memory sticks. Since 2011, a total of 12 privacy breaches have been reported across CSC regarding the loss of USB devices containing offender information.

During interviews with institutional chiefs of informatics, the audit team found that at eight of the sites visited, a list existed to track who was given a USB device. A concern was raised by the chiefs of informatics that even with maintaining a list, the lack of serial numbers or other individual identifiers on the memory sticks made it difficult to ensure that the individual assigned to the USB device still had it in their possession. It was also difficult to ensure that staff members were not inappropriately using these memory sticks to store and transport offender information. The audit team found that with the exception of two institutions, most sites were providing staff with USB sticks without determining their need for it. The chiefs of informatics at these two sites did state that they did not see a need for many USB devices since staff were able to use an encrypted laptop when away from the institution and were able to remotely connect to the institution's network.

To further minimize the possible privacy concerns with the information being stored on regular USB devices, institutions were slowly acquiring encrypted USB devices. These devices, if lost, would ensure that the private information stored on them is adequately safeguarded. That said, due to the costs of these encrypted USB devices, most sites visited had purchased very few and typically were only providing them to wardens and deputy wardens.

Infrastructure layout within federal institutions further challenges the protection of the information.

While on site, the audit team asked institutional staff if, in their opinion, they had any concerns regarding the privacy of offender information at their site. One common theme which stood out was that the physical infrastructure of the institution sometimes impedes the institutional staff members' ability to ensure that privacy of offender information is always maintained. During

the observations conducted at the institutions by the audit team, a number of privacy issues caused by infrastructure challenges were noted.

The first infrastructure concern found related to the requirement for shared offices between disciplines within the institutions. At many sites, as the offender population continues to grow, due to limited administrative areas, staff are sharing offices and work areas between disciplines in order to maximize space. For example, at one site, the audit team found that in the units, behavioural counsellors and psychologists were sharing a single office. In cases where offices were being shared, concerns were raised that maintaining privacy and ensuring need-to-know was complicated as the other discipline did not have a need-to-know although the information was easily accessible.

Another infrastructure concern that the audit team found related to inmate waiting areas in both administrative areas and health care units within some institutions. Due to the lack of adequate space, offender waiting areas were sometimes in locations where they could easily overhear what was being discussed regarding specific offenders. In addition, health care privacy concerns were raised to the effect that due to security issues at some sites, offenders would be forced to state issues to a nurse through a window before they would be brought back for an individual assessment, allowing others in the waiting area to overhear. This was also noted as a concern during the distribution of medication, as discussions between offenders and nurses could not occur at these times without other offenders overhearing the entire conversation. A similar finding was included in the 2012 *Audit of Medication Management*.

The third common infrastructure concern noted at many institutions involved the correctional officer security posts at the institutions. Challenges were noted in most units, whether they were the older style living units or newer open concept ones, that correctional officers had to be extremely cognizant of what information they were reviewing or discussing as people without a need-to-know could learn or overhear this private information. For example, at the older style living units, officers raised concerns that as the entire security office is surrounded by windows, they commented, that offenders would sometimes read what the officer was typing into the computer. In the newly constructed living units, correctional officer control posts are now open concept with no barriers or windows between officers and offenders. While the audit team was told that this open concept style works well from a security standpoint, and improves interaction between offenders and staff, the open concept does require staff to be more cognizant in order to maintain privacy of information. As there are no walls, voices travel much easier and conversations between correctional officers at the control posts are easily heard by offenders in the unit. Furthermore, information, including the unit count board is more easily viewed by offenders within the unit. That said, staff in these units seemed to be aware of this challenge and would typically hold conversations and write private reports in a back office away from the individuals who do not have a need-to-know.

While infrastructure challenges may hinder the privacy of information, many of the institutional employees interviewed during the site visits seem to be aware of the limitations they were facing. At many institutions, the infrastructure concerns noted were typically raised during interviews by institutional staff. That said, as the infrastructure challenges will continue to exist, CSC must

ensure that institutional employees are cognizant of the limitations that the infrastructure provides and ensure that employees are aware to adapt to these challenges to ensure the privacy of information is maintained.

Printers and photocopiers were located in easily accessible areas and sensitive offender information was found to be vulnerable.

In order to reduce costs and minimize waste, CSC has recently adopted a policy to replace aging printing devices with new multifunction units, while increasing the ratio of staff to printers to eight to one. In making this decision, printers will now be shared amongst more staff and across more disciplines, thus increasing the likelihood that individuals without a need-to-know may inadvertently access personal information on an offender.

Since 2011, a total of 59 breaches of offender privacy relating to the inadvertent release of offender paper information have been reported across CSC, with many of these breaches being caused by errors in handling printed material. Interviewees stated that human error causes some breaches when sharing information with offenders as when a report is printed, an additional page from a report related to a different offender can sometimes be attached to it. In fact, during observations made at the 15 sites, the audit team checked 167 common printers and photocopiers to confirm that no documentation was left behind or not collected. The audit team found 14 cases where printouts, which appeared to be related to personal information about an offender, were left on a common printer or photocopier. When this information is left on the printer, there is a risk that it could accidentally get shared or that someone who does not have a need-to-know for this information accidentally obtains or reads it. In many instances where printouts of sensitive information were left on the printers, the interviewees stated that the printer was in a staff only area with no unsupervised offender access. That said, as previously stated in Section 4.2.2, not all staff has a need-to-know about every offender and printouts should be safeguarded to the same level whether or not offenders have access to the printers. This issue regarding printouts becomes even more relevant due to different disciplines sharing the same printer.

The audit team found that at eight sites, the institutions were trying to implement methods to minimize the risk of printed documents inadvertently being shared with individuals without a need-to-know. The audit team found that in four institutions, shared printers typically printed information to assigned trays, so that information belonging to others would not all get piled together. Meanwhile, at four other sites, staff were taking advantage of the opportunity to "secure print" a document. By doing this, the person printing a document would be required to physically go to the printer and enter a PIN number prior to the printer dispensing the spooled documents. While this does minimize the risk of printouts from various individuals being left on the printer, it is a setting which the user controls, and thus can be easily disabled. In most sites which were using the secured print option, staff stated they would do it for information which they deemed to be of a more sensitive nature.

Conclusion

The audit team found that overall CSC had processes in place to report privacy breaches and for those breaches that were known, privacy risk assessments were completed. In addition, the hard drives of all CSC laptops are encrypted. Furthermore, staff possess a basic knowledge of the need-to-know principle.

While the audit team understands that CSC is hindered by both infrastructure challenges and human error, there were however a number of areas audited that require CSC attention to ensure the privacy of offender information is better maintained. These areas include:

- ensuring that the need-to-know principle is consistently interpreted and applied across CSC;
- mechanisms should be used to identify offender report copies;
- institutions should ensure that appropriate methods to dispose of offender information are used;
- non-encrypted and untracked portable media devices should not be used throughout the institutions; and
- institutions should ensure that personal offender information is collected from printers and photocopiers in a timely manner.

Recommendation 2[6]
The Assistant Commissioner, Policy, should provide additional clarification to all CSC staff to support the need-to-know principle. RDC's should ensure that institutional and district management have in place controls and mechanisms to ensure that the need-to-know principle is understood and applied as appropriate.

[6] Recommendation requires management's attention, oversight and monitoring.

Management Response

A/ACP, ACCOP and RDCs agree with this recommendation

Actions include:

- *The development of an NHQ ATIP Bulletin explaining the "need-to-know" principle to provide clarification to all staff on access to personal information for their work. The Bulletin has been sent to RHQ ATIP Liaisons for distribution to Operational units and their staff. The Bulletin has also been posted on the NHQ ATIP Infonet site. This action has been completed.*
- *GEN-NHQ ATIP has developed a series of notices to form "pop-up" notices for staff computers. NHQ IT has been contacted to explore the possibility of having notices used as reminders to staff on how to safeguard personal information and to reinforce the "need to know" principle.*
- *ACCOP has reviewed and promulgated CD-701 (Information Sharing) that includes the "need-to-know" principle. This action has been completed.*
- *For a list of all actions associated with this recommendation, please refer to the Management Action Plan. Full implementation for Recommendation 2 by July 31, 2014.*

Recommendation 3[7]

Regional Deputy Commissioners should ensure that Institutional Heads have processes in place to minimize, or reduce, the occurrences of privacy breaches of offender information by implementing various processes which address the areas of weakness identified in the report as well as any other areas they determine as requiring attention.

Management Response

A/ACP and RDCs agree with this recommendation.

Actions include:

- *Following the distribution of the ATIP Privacy Breach quarterly reports, the RDC will provide information regarding actions taken to prevent further incidents of a similar nature and this will be communicated regularly with the regional management team.*
- *Training and Awareness sessions will be delivered to ensure that all employees are trained and aware of the various types of breaches and their responsibilities vis-à-vis reporting of breaches. The training will include managers, so that they will be aware of their responsibilities when breaches are reported.*
- *Full implementation for Recommendation 3 by July 31, 2014.*

[7] Recommendation requires management's attention, oversight and monitoring.

5.0 Overall Conclusion

Overall, while tools and processes are in place to protect the privacy of offender information, areas for improvement exist. The management framework needs to be strengthened in order to ensure that the privacy of offender information is maintained. CSC's privacy framework requires updating to further clarify roles and responsibilities, to ensure the reporting of privacy breaches and to improve overall awareness. To ensure CSC is better able to protect private offender information, the need-to-know principle should be reviewed and controls surrounding the protection of offender information must be in place and abided to by staff.

Management Response

- *A/ACP agrees with the overall audit findings and recommendations as presented in the audit report.*
- *A/ACP has prepared a detailed Management Action Plan to address the issues raised in the audit report.*
- *The Management Action Plan will be implemented by July 31, 2014. Some actions will be conducted on an ongoing basis (such as ATIP training and awareness sessions).*

Annex A: Audit Objectives and Criteria

Objective	Criteria
Objective #1 To provide reasonable assurance that the management framework in place ensures the privacy of offender information and is in accordance with various acts and legislation.	**1.1 –Policy and Procedures** 1.1.1 Guidelines and bulletins to support privacy of offender information are in place and have been communicated to all staff. 1.1.2 Guidelines, policies and frameworks exist and are consistent with Government of Canada policies and national acts and legislation related to privacy of information.
	1.2 –Roles and Responsibilities 1.2.1 Roles and responsibilities related to the governance and duties related to ensuring the privacy of offender information are clearly defined, understood and documented.
	1.3 –Training and Awareness 1.3.1 Training related to maintaining the privacy of offender information has been developed, provided and taken by CSC employees. 1.3.2 Staff understand and maintain the various principles as they relate to the privacy of offender information.
	1.4 –Reporting of Privacy Breaches 1.4.1 A formalized process exists and is being followed to allow both staff and offender to report privacy breaches of offender information.
	1.5 –Monitoring and Reporting 1.5.1 Management monitors the privacy breaches reported to ensure that reoccurring breaches are minimized and that the fundamental causes are corrected.
Objective #2 To provide reasonable assurance that CSC is ensuring that the privacy of offender information is maintained as required by the applicable legislation, acts and departmental frameworks.	**2.1 –Analysis of Incident** 2.1.1 Institutions are completing privacy risk assessments, are providing and implementing corrective actions where needed following any privacy breach of offender information.
	2.2 –Need-to-Know 2.2.1 The need-to-know principle is being followed and adhered to in accordance with CSC's privacy frameworks.
	2.3 –Safeguarding of Offender Information 2.3.1 Controls are in place and being abided by employees to ensure that offender information is upheld and safeguarded throughout the institutions.

Annex B: Location of Site Examinations

Region	Sites
Atlantic	• Dorchester Institution • Shepody Healing Centre • Springhill Institution
Quebec	• Centre Régional de Réception • Centre Régional de Santé Mentale • Établissement Archambault
Ontario	• Beaver Creek Institution • Fenbrook Institution • Warkworth Institution
Prairies	• Bowden Institution • Edmonton Institution • Edmonton Institution for Women
Pacific	• Ferndale Institution • Fraser Valley Institution • Pacific Institution

Annex C: Audit Approach and Methodology

Interviews: 211 interviews with staff were conducted either in person, by videoconference or by teleconference. An additional 16 interviews with Inmate Welfare Committees were conducted. Interviews took place across all five regions, including National Headquarters, Regional Headquarters and selected institutions.

Review of Documentation: Relevant documentation such as legislation, bulletins, policy documents and guidelines, privacy frameworks, procedure manuals, annual reports and meeting minutes including Privacy Committee Meetings minutes were reviewed.

Observations: Observations were conducted in correctional manager's offices, common hallways, case management offices, health care, psychology, records, visits and correspondence, programming, admission and discharge, security intelligence offices, living units and segregation to determine if safeguarding measures were implemented to ensure any information pertinent to the offender privacy was protected.

Site Selection: Various factors were used in the selection of institutions for this audit. These included institutional security levels and capacity and the geographical location of the institutions to ensure selection of both urban and rural sites and other site irregularities.

Analytical Review: An analytical review was conducted throughout the audit, to determine trends for the privacy of offender information.

Annex D: Location of Interviewees

REGION	SITES
NHQ	• Director, and Deputy Director, ATIP • Director General, Security Branch • Director, Information Management • Director, Information Technology • OMS Data Quality and Support Team
RHQ	• Regional Access to Privacy and Information Liaison Officer
Institutions – Formal Interviews	• Warden/Executive Director • Deputy Warden • Assistant Warden, Management Services • Chief of Informatics • Chief of Administrative Services
Institutions – Interviews Conducted during walk-arounds	• Manager, Assessment and Interventions • Security Intelligence Officer • Correctional Manager • Correctional Officer • Unit Assistants • Parole Officer • Chief of Nursing/Nurse • Chief of Psychology/Psychologist • Grievance Coordinator • Records Clerk • Inmate Welfare Committee

Annex E: Acronyms and Abbreviations

ATIP	Access to Information and Privacy
CD	Commissioner's Directive
COSO	Committee of Sponsoring Organizations
CSC	Correctional Service Canada
DS	Departmental Security
FPS	Fingerprint Section
IM	Information Management
ITSEC	Information Technology Security
NEOP	New Employee Orientation Program
NHQ	National Headquarters
OMS	Offender Management System
OPC	Office of the Privacy Commissioner of Canada
OPI	Office of Primary Interest
PAPR	Parliamentary Affairs and Public Relations
PIA	Privacy Impact Assessment
PMF	Privacy Management Framework
PRA	Privacy Risk Assessments
RHQ	Regional Headquarters
TB	Treasury Board

Glossary

The Access to Information Act: gives Canadian citizens, permanent residents, or any person or corporation present in Canada a right to access information that is contained in government records. The Act is intended to complement existing procedures for access to government information such as Open Government initiatives[8].

Burn boxes: boxes located in individual work areas to place protected private information to be disposed of by a contract company at a later time.

Count board: reflects the names, FPS numbers and cell locations of all inmates currently in the institution and the names and FPS numbers of all inmates not physically in the institution (i.e. temporary absence, outside hospital, unlawfully at large, etc.) is maintained.

Double bunking: cell designed for one inmate, but housing two inmates.

Fingerprint Section (FPS): number assigned to each offender by the Royal Canadian Mounted Police used as the standard offender identifier for the Service[9].

Inmate Welfare Committee: the Inmate Committee will make recommendations to the Institutional Head on decisions affecting the inmate population, except decisions relating to security matters[10].

Offender Management System (OMS): computerized file management system that manages information on federal offenders throughout their sentence.

Personal Information: information about an identifiable individual that is recorded in any form such as an individual's race, age, fingerprints, medical, criminal or employment history, identifying number or symbol (i.e. PRI, FPS).

Portable Storage Device: a small hard drive designed to hold any kind of digital data.

Privacy Act: this Act imposes obligations on some 250 federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. The Privacy Act also gives individuals the right to access and request correction of personal information about themselves held by these federal government organizations[11].

Privacy Breach: the improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information which results from poor personal information management.

[8] http://www.tbs-sct.gc.ca/atip-aiprp/tools/administration-application-eng.asp.
[9] Commissioner's Directive 703, Sentence Management, para 12.
[10] Commissioner's Directive 083, Inmate Committees para 10.
[11] http://www.priv.gc.ca/leg_c/leg_c_a_e.asp.

Type of Privacy Breach
TYPE 1: Theft or loss of records (hard copy file or document)
TYPE 2: Theft or loss of electronic assets (i.e. laptops, briefcases, USBs containing personal information, etc.)
TYPE 3: Disclosure of information due to human error in handling hard copies or electronic files (e.g. misdirected emails)
TYPE 4: Electronic access to information without a need to know
TYPE 5: Disclosure of information to the media
TYPE 6: Disclosure of victim information
TYPE 7: Disclosure of information (verbally or in writing) to outside parties

Privacy Breach Guidelines: proposes the reporting and evaluating of breaches to personal information.

Privacy Commissioner of Canada: an Officer of Parliament who reports directly to the House of Commons and the Senate. The Commissioner is an advocate for the privacy rights of Canadians and powers include: Investigating complaints, conducting audits and pursuing court action under two federal laws; publicly reporting on the personal information-handling practices of public and private sector organizations; supporting, undertaking and publishing research into privacy issues; and promoting public awareness and understanding of privacy issues[12].

Privacy Management Framework (PMF): consistent with the CSC priority of strengthening CSC management practices, the PMF ensures that privacy is a core consideration in the management of personal information, so that policy and program development, management practices and service delivery reflect the spirit and requirements of the *Privacy Act*, and ensuring legal obligations are met in an environment of change[13].

Privacy Risk Assessment: a document used to ascertain the level of risk of the breach and measures to be taken[14].

Reporting Authority: NHQ Division/Sector that the Reporting Manager notifies of the breach (one or more of: Information Management (IM), IT Security (ITSEC), Departmental Security (DS), Parliamentary Affairs and Public Relations (PAPR) and the Access to Information and Privacy Division (ATIP)).

Shredding Bins: locked boxes to hold information for disposal, with the contents emptied and destroyed on a regular basis by a licensed information disposal company.

Treasury Board Secretariat Policy on Government Security: this policy aims to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management[15].

[12] http://www.priv.gc.ca/au-ans/index_e.asp.
[13] CSC Privacy Management Framework, p. 4.
[14] CSC Guidelines for Privacy Breaches, p. 4.

USB Memory Stick: USB memory sticks are convenient storage devices that allow for easy transfer of data from one computer to another.

[15] Policy on Government Security, para 5.1.