Office of the
Privacy Commissioner
of Canada

AUDIT OF SELECTED RCMP OPERATIONAL DATABASES

Audit Report of the
Privacy Commissioner of Canada

Section 37 of the *Privacy Act*

FINAL REPORT

2011

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190
Follow us on Twitter: @privacyprivee

© Minister of Public Works and Government Services Canada, 2011

Cat. No. IP54-42/2011
ISBN 978-1-100-53857-0

This publication is also available on our website at **www.priv.gc.ca**.

Table of Contents

Main Points

WHAT WE EXAMINED

Canada's law enforcement and criminal justice community relies upon an extensive network of database systems to help enforce laws, prevent and investigate crime, and maintain peace, order and security. As Canada's national police service, the Royal Canadian Mounted Police (RCMP) has provided leadership in identifying needs and developing information systems and related services and making them available to the broader community.

Due to their importance and extensive use by the RCMP and other members of the larger law enforcement community, our audit focused on two of these systems: the Canadian Police Information Centre (CPIC) and the Police Reporting and Occurrence System (PROS). CPIC provides computerized storage and retrieval of information on crimes and criminals. PROS is the RCMP's primary operational records management system.

The audit examined RCMP policies and procedures governing the access and use of CPIC, the policies and procedures to remove personal information contained in PROS that is no longer required, the RCMP's review practices for compliance with the terms and conditions of use for both CPIC and PROS, and the management of user access to PROS.

WHY THIS ISSUE IS IMPORTANT

Both CPIC and PROS contain extensive sensitive personal information that, if improperly used or disclosed, could have a significant impact on the rights and freedoms of individuals as well their reputations, employability and safety. A security breach may also compromise ongoing police investigations. The RCMP reports annually on security breaches related to the CPIC system. Many of these breaches have involved unauthorized access to and inappropriate use of personal information, with potentially significant privacy implications for the individual whose information was accessed.

The RCMP has also found that certain police agencies were disseminating the details of convictions, discharges or pardons to employers without the informed consent of the prospective employee, in contravention of CPIC policy.

Information in these databases is available to a wide range of users throughout the law enforcement community, both in the office and on the road. For example:

- CPIC data banks include, but are not limited to, information on: drivers' licences and vehicle plates, stolen vehicles and boats, warrants for arrest, missing persons and property, criminal history records, fingerprints, firearms registration and missing children. CPIC holds more than 10 million records and processed more than 200 million queries through 40,000 access points in 2009.
- PROS is a complete occurrence and records management system containing information on individuals who have come into contact with police, either as suspects, victims, witnesses or offenders, from initial occurrence to final disposition. PROS is used by the RCMP and 23 police partner agencies as their operational records management system. About 1.6 million occurrence files are processed per year.

The RCMP is responsible for the storage, retrieval and communication of shared operational police information to accredited criminal justice and other agencies involved with the detection, investigation and prevention of crime. It has an obligation to protect the privacy of individuals with respect to the personal information in its care.

WHAT WE FOUND

Canadian Police Information Centre

The RCMP has developed and implemented policies and procedures to protect the personal information of Canadians being accessed and used in the CPIC database. Although privacy breaches have occurred, they are relatively rare and mechanisms are in place to investigate them and for action to be taken pursuant to those investigations. Many of the breaches involved users querying CPIC for personal reasons. Investigations that conclude there was a misuse of CPIC can result in a change in CPIC policy, a reprimand, suspension or dismissal.

The RCMP has established memoranda of understanding (MOUs) to govern the use of CPIC by agencies with limited law enforcement powers or roles complementary to law enforcement. However, the RCMP had yet to formally establish MOUs with approximately 25 percent of the police agencies that access CPIC.

Regular audits are performed to examine security screening of personnel, security at the CPIC terminal and/or interface site, and to ensure that policy and guidelines in the CPIC reference manual are adhered to by all agencies, including the RCMP. This monitoring regime is intended to ensure that all users are compliant with the requirements, including privacy principles, outlined in CPIC policy.

The RCMP was made aware of recent incidents where certain police agencies were disseminating criminal record information obtained from the CPIC system that was in direct contravention of CPIC policy, the *Criminal Records Act*, the *Youth Criminal Justice Act* and the Ministerial Directive on the Release of Criminal Records. A number of agencies were disseminating the details of convictions, discharges or pardons to employers without the informed consent of the prospective employee, and without confirming identity by means of a fingerprint comparison. In response to these disclosures, in November 2009, the RCMP issued a directive to agencies using CPIC noting that not all entities were complying with established policies and procedures regarding the use of the CPIC system. This was further strengthened in August 2010 when the Minister of Public Safety issued a directive clarifying the conditions under which criminal record information maintained in CPIC may be used and disclosed.

Police Reporting and Occurrence System

The RCMP has developed a comprehensive set of policies, standard operating procedures and agreements to ensure the use of PROS respects the principles set out in the *Privacy Act*. However, information purging, better access management, systematic reviews and more effective access to user activity logs are needed to ensure that PROS users are complying with RCMP policies and procedures as well as provincial and federal privacy legislation.

The RCMP has developed policies and standard operating procedures that set out how long personal information may be retained in PROS before it must be sequestered or deleted. However, we found that personal information is being retained longer than required, in contravention of the *Privacy Act*. Further, we found the RCMP has no process for the removal of access to records related to pardoned offences, or records related to wrongful convictions.

There is no active review of PROS user accounts. While the RCMP's PROS policy requires that a user's access be revoked when no longer required to perform job functions or after 14 months of inactivity, we found there were over 1,000 users with active accounts who had not accessed PROS for a period of 14 months or longer. We also found the process used to review user activity on PROS to be cumbersome, rendering reported incidents of misuse difficult to investigate.

The RCMP was unable to demonstrate that it systematically reviews PROS users to ensure that the personal information contained in PROS is used in accordance with the governing policies.

The RCMP has responded to our findings. Its responses follow our recommendations throughout this report.

Introduction

BACKGROUND

1. The Royal Canadian Mounted Police (RCMP) is Canada's national police service. It has approximately 30,000 members and employees whose mandate includes preventing and investigating crime; maintaining peace and order; enforcing laws; contributing to national security; and protecting state officials, visiting dignitaries and foreign missions.

2. The RCMP enforces federal laws across the country, and provincial/territorial laws in all provinces (except Ontario and Québec) and the territories, as well as nearly 200 municipalities, under the terms of policing agreements with those jurisdictions. The RCMP also provides investigative and operational support services to more than 500 Canadian law enforcement and criminal justice agencies.

3. CPIC and PROS are two of the databases the RCMP relies on in support of these services.

4. CPIC provides computerized storage and retrieval of information on crimes and criminals. CPIC is widely used by the law enforcement and criminal justice community. In 2009, CPIC held 10 million records and processed over 200 million query requests through 40,000 points of access. It allows more than 80,000 law enforcement officers to connect to the central computer system from more than 3,000 police departments, RCMP detachments and federal and provincial agencies across the country.

5. CPIC data banks include information on drivers' licences and vehicle plates, stolen vehicles and boats, warrants for arrest, missing persons and property, criminal history records, fingerprints, firearms registration, missing children and other subjects. CPIC has been described as the backbone of the criminal justice system. It provides the law enforcement community with access to a wide range of information on Canadians. The courts, parole boards and government departments and agencies such as Correctional Service Canada and the Canada Border Services Agency, also use CPIC for a variety of purposes.

6. PROS is the RCMP's police records management system. It is a records management system containing information on individuals who have come into contact with police, either as a suspect, victim, witness or offender. PROS was introduced in 2003 to record all aspects of an investigation, from the moment an occurrence is reported to final disposition if the matter goes to court. PROS is used by both the RCMP and 23 police partner agencies as their operational records management system. Police partner agencies are smaller agencies (typically fewer than 300 officers) that do not have their own electronic records management system.

EXHIBIT 1: AN EXAMPLE OF HOW CPIC AND PROS ARE USED

An RCMP officer stops a car for speeding. The officer first runs a query in CPIC on the vehicle and the driver to see if the vehicle is stolen or if there are any outstanding warrants. The officer might then search PROS to see if the vehicle or person had been involved in other incidents. An occurrence record is created in PROS to record the event. The record would be updated later to include subsequent events—any charges laid and their disposition.

FOCUS OF THE AUDIT

7. The audit objective was to determine whether the RCMP is adequately managing the personal information contained in the CPIC and PROS databases.

8. We did not examine how the information in these databases influenced decisions as part of the day-to-day operations of the RCMP. Further, the audit did not look at the safeguards put in place by users of CPIC and PROS other than the RCMP. Information contained in CPIC is shared internationally via Interpol and with U.S. law enforcement agencies such as U.S. Customs and Border Protection. The audit did not examine the safeguards surrounding those sharing arrangements.

9. Additional details regarding the audit objective, scope, approach and criteria are available in the **About the Audit** section of this report.

Observations and Recommendations

CANADIAN POLICE INFORMATION CENTRE (CPIC)

10. The RCMP Commissioner is the overall governance authority for CPIC. The CPIC Advisory Committee provides advice and recommendations to the Commissioner for establishing the scope of the CPIC program and determining eligibility for participating agencies. The CPIC Advisory Committee is made up of representatives from major police departments as well as federal and provincial law enforcement representatives.

11. The RCMP is responsible for hosting the CPIC database, establishing controls and ensuring that monitoring is undertaken. Depending on the mandate of the agency accessing the CPIC database, the RCMP will set up an appropriate level of access based on a recommendation from the CPIC Advisory Committee. To assure compliance with the terms and conditions under which access was granted, the RCMP oversees an audit program to ensure reviews are undertaken on a regular basis. These audits examine, among other issues, whether the mandatory data that must be entered into the CPIC database is complete and whether there is adequate security around access to the system. However, the accuracy and timeliness of the information entered into CPIC is deemed to be the sole responsibility of the agency making the entry.

12. Given the sensitivity of the personal information contained in this database, we expected to find that the RCMP had policies and procedures in place to ensure the appropriate level of access is provided to CPIC users. To ensure there is no unauthorized disclosure of personal information, we expected to find that the RCMP had established and was verifying user compliance with the rules governing appropriate access and use of this database.

13. We examined whether the RCMP:
    - has policies and procedures in place to govern the access and use of the personal information contained CPIC; and
    - ensures that CPIC is monitored for user compliance with the terms and conditions of access and use.

Policies and procedures to protect the personal information accessed from CPIC are well established

14. When an agency requests access to the CPIC system, the request is reviewed by the CPIC Advisory Committee and, if approved, is forwarded to the RCMP so the access request can be processed. There are a number of different levels of access, which are granted based on the mandate of the requesting agency.

15. Once CPIC access has been approved for an agency, policy requires the RCMP to conduct a security evaluation to ensure that the technical infrastructure of the agency is adequate. We examined this evaluation process and found that many essential elements to ensure a secure environment were present in the requirements. These include physical security, authentication of users and requirements for secure network configurations. Although we were satisfied with the complete and robust nature of the security

evaluation framework, the RCMP was unable to demonstrate that security evaluations had been completed for all agencies that had access to CPIC.

16. Due to the volume of data contained in CPIC and the large number of users, policies and procedures along with written agreements have been put in place to protect the privacy of individuals. MOUs containing privacy protection provisions establish the terms and conditions governing the use of CPIC by the member agencies. The RCMP has assembled policies and procedures into a single document: the *CPIC Reference Manual* (the Manual).

17. The Manual contains the policies and procedures used to govern the overall operations of CPIC and it addresses the fair information principles embodied in the *Privacy Act*. It includes the principles of data use, collection, accuracy, safeguarding, retention and disclosure.

18. The RCMP was made aware of recent incidents where certain police agencies were disseminating criminal record information obtained from the CPIC system in direct contravention of CPIC policy, the *Criminal Records Act*, the *Youth Criminal Justice Act* and the Ministerial Directive on the Release of Criminal Records. The RCMP informed us that a number of agencies were disseminating the details of convictions, discharges or pardons to employers without the informed consent of the prospective employee and without confirming identity by means of a fingerprint comparison.

19. In response to these disclosures, the RCMP issued a directive in November 2009 to agencies using CPIC noting that not all entities were complying with established policies and procedures regarding the use of the CPIC system. Then, in August 2010, the Minister of Public Safety issued a directive clarifying the conditions under which criminal record information maintained in CPIC may be used and disclosed.

20. A written agreement such as an MOU governs compliance with CPIC policy. The RCMP has MOUs in place with member agencies to govern access to CPIC. Although the MOUs differ somewhat depending on which category the agency belongs to or, in some cases, the specific mandate of a given agency, all MOUs include procedures to be followed with respect to the handling of personal information contained in the database. Personnel clearance requirements for CPIC access, including criminal records checks and mandatory training, are defined. The MOUs set out the procedures to be followed when disseminating or sharing information from CPIC, and require the agency to report any and all known or suspected breaches. The MOUs state that the agency is expected to comply with applicable provincial and federal access-to-information and privacy laws. Any agency that is found not in compliance may have its CPIC privileges revoked.

21. We found the RCMP had established MOUs with agencies that have limited law enforcement powers, such as the Canada Border Services Agency, Canada Revenue Agency, Citizenship and Immigration Canada, Correctional Service Canada and the National Parole Board. As well, agencies with roles complementary to law enforcement, such as Passport Canada, Transport Canada and the Insurance Bureau of Canada had MOUs in place. We noted that the MOUs in place are renewed periodically, at which time the agency's requirement for access is reassessed and either continued or adjusted.

22. However, we found the RCMP had yet to formally establish MOUs with approximately 25 percent of the police agencies that access CPIC. Previously, these agencies were not required to have MOUs, as their access to CPIC was granted based on their core policing role. During the course of our audit, the RCMP was negotiating terms and conditions with police agencies that did not yet have MOUs in place.

23. RECOMMENDATION

CPIC should set a clear timeframe for establishing MOUs, which include privacy provisions with all entities.

RCMP response:

The CPI Centre is currently and actively in negotiation with the final 25 percent of the agencies that have yet to sign an MOU as directed by the Deputy Commissioner, Policing Support Services in November 2010. As expected, a template approach to MOUs does not necessarily apply to all cases and differences are being discussed in order to have MOUs in place by March 31, 2012.

24. In order for users of an approved agency to be granted access to CPIC, CPIC policy requires that a user first receive appropriate training. We found the training program contains modules that instruct users on their obligations toward privacy and what constitutes an acceptable use of CPIC. As well, users are informed that CPIC transactions must be for legitimate use and must not be used for personal reasons, and that reported violations of CPIC policy and procedures will be investigated. Consequences or penalties resulting from investigations range from requirements for reinforcement training to fines, suspension and termination of employment.

25. We examined the controls in place to ensure that users are authorized to access CPIC. We found that CPIC has an ongoing IT risk mitigation strategy. This strategy includes a requirement that member agencies implement enhanced security by requiring CPIC users to use both a physical token and a password to log on to the CPIC system. This is referred to as strong identification and authentication.

26. However, we found that 33 percent of CPIC member agencies have not yet implemented this user authentication procedure due to technical constraints in their infrastructures. We noted that the RCMP had established a target date of April 2009 for these agencies to deploy the required security measures. We found that the RCMP has been monitoring the progress of delinquent agencies to implement the required level of security.

A monitoring regime is in place to govern proper use

27. The information contained within CPIC is used by police services and other agencies for investigation and enforcement actions that impact thousands of Canadians every day. For this reason, it is important to ensure that CPIC standards and practices are followed to assure the information contained therein is valid and accurate, and that information-handling procedures comply with applicable privacy legislation.

28. The maintenance of accurate up-to-date information is the responsibility of the CPIC agency contributing such information. We found that the RCMP sends a validation report to each contributing agency every month to review the integrity of the data. Agencies are required to verify the validity and accuracy of their entries and to make any necessary adjustments.

29. We found that audits of CPIC member agencies are conducted by the RCMP (except in Ontario and Québec where the audits are performed by the Ministry of Community Safety and Correctional Services and the Sûreté du Québec, respectively) to ensure compliance with the validation process and to determine if an agency is compliant with the privacy principles outlined in CPIC policy. Standard procedures, tools and reporting are used. CPIC policy requires that an audit to confirm compliance with policy and procedures be completed for each agency at least once every four years. Any new agency is audited

within one year of being granted access to CPIC. In the fiscal year 2009–10, 477 CPIC audits were conducted.

30. The auditors look for the quality and integrity of records entered in the CPIC system and assess the system knowledge and proficiency of the agency personnel. Furthermore, auditors examine security screening of personnel, security at the CPIC terminal or interface site, and ensure that policy and guidelines in the CPIC reference manual are adhered to by all agencies.

31. Upon completion of the audit, the auditors compile and distribute a summary report to the CPIC Advisory Committee outlining their findings. A report of the number of audits conducted by region is published in the CPIC annual report. A follow-up verification is conducted within a few months of the completion of the audit to ensure that deficiencies have been addressed.

32. We also found that the RCMP tracks reported CPIC security breaches. The RCMP monitors investigations of breaches of CPIC security reported by police departments and individuals. We found that reported security breaches are relatively rare and that these incidents are investigated. Audit activities have been responsible for detecting approximately 10 percent of CPIC breaches, while remaining breaches have been identified through ongoing reviews or complaints. There are more than 200 million CPIC queries annually and, in 2009, there were 280 reported breaches. Of those, investigations determined that 24 were founded and 86 were unfounded, while 170 remained under investigation. Many of the breaches involved querying CPIC for personal reasons. Security breaches can result in a change in CPIC policy, a reprimand, fines, suspension or dismissal of the employee involved.

POLICE REPORTING AND OCCURRENCE SYSTEM (PROS)

33. PROS is a police records database used by the RCMP and 23 police partner agencies as their operational records management system. Partners are smaller agencies (fewer than 300 officers) that do not have their own electronic records management system. The RCMP provides access to the PROS database and houses the data. Approximately 1.6 million occurrence files per year are processed using PROS.

34. PROS was introduced in the fall of 2003 and was in full production nationally by the summer of 2005. PROS is used to record all aspects of an investigation, from the moment an occurrence is reported to final disposition if the matter goes to court. It contains information on individuals who have come into contact with police, either as suspects, victims, witnesses or offenders.

35. Given the sensitivity of the personal information contained in this database, we expected to find that the RCMP had policies and procedures in place to ensure that the personal information contained in PROS is handled in accordance with legislative requirements for retention and disposal, and is adequately protected from unauthorized access. Retention policies and procedures are drawn from governing legislation such as the *Criminal Records Act* and the *Youth Criminal Justice Act.*

36. We examined whether the RCMP:

- established policies and procedures to remove personal information contained in PROS that is no longer required;
- is adequately managing access to PROS; and
- ensures that the use of PROS is monitored for compliance with RCMP policies and procedures to protect personal information.

Personal information is being retained longer than required

37. We found that the RCMP has developed policies and standard operating procedures for PROS that set out how long information may be retained before the information must be sequestered or deleted in accordance with governing legislation.

38. There are legislative requirements to sequester certain information when the retention period for that information has been met. Sequestering involves placing records into a special repository that has highly restricted access. Types of information that are sequestered include details relating to absolute or conditional discharges and pardons.

39. Legislation requires that all records created in PROS be purged when the retention period for each category of information has expired. Prior to deletion, records are evaluated to determine if they should be archived with Library and Archives Canada.

40. We examined the procedures governing the retention of personal information in PROS and found that the database was designed to automatically purge occurrences once they reach their disposition date unless they have archival value. We found the RCMP had disabled this function. As a result, personal information of an individual whose data should have been purged can still be readily accessed from the PROS database.

41. The RCMP informed us this was done so that statistical information can be extracted from PROS. As a result, occurrences that should be purged because they have reached the end of their retention period are not removed.

42. RECOMMENDATION

The RCMP should purge the required data from PROS so that it is in compliance with the *Privacy Act*.

RCMP response:

The RCMP agrees and will take immediate steps to rectify this situation.

43. **Access to pardoned offences is not removed as required.** While examining purging procedures mandated by the *Criminal Records Act* and *Youth Criminal Justice Act*, we found that the RCMP has not yet implemented a process to remove records related to pardoned offences from the PROS database.

44. When a pardon is issued, the records relating to that offence should no longer be accessible from PROS. We found that if the name of an individual with a pardoned offence were to be queried on PROS, the details of the pardoned offence may appear.

45. It is important to Canadians who have received a pardon that the information not be inappropriately disclosed. Doing so could hinder their opportunities to get a job, travel, study or volunteer. The *Canadian Human Rights Act* prohibits discrimination based on a pardoned record.

EXHIBIT 2: DISCLOSURE OF PARDONED AND DISCHARGED OFFENCES

There are exceptions where the existence of a pardoned or discharged offence may be disclosed. These exceptions are defined in the *Criminal Records Act*. The name, date of birth and last known address of the subject of a pardoned or discharged offence can be disclosed to a police force to aid in an investigation if a fingerprint matching that of the subject is found at the scene of a crime. This same information may also be released to a police force to identify a deceased person or person suffering from amnesia. The existence of a conviction for a sexually based offence may be disclosed in the context of a Vulnerable Sector Search. This type of search may be requested by an authorized representative of an organization responsible for the well-being of vulnerable persons to verify an applicant who has applied for a paid or volunteer position, and who has consented in writing to the verification and disclosure.

46. **No procedure to remove wrongful convictions.** While there have been no known cases of wrongful convictions that fall under the control of the RCMP since PROS went into full production in 2005, the RCMP does not have a procedure to remove records related to wrongful convictions. Although standard operating procedures exist on sequestering information other than pardons as well as processing conditional and absolute discharges, we found that the RCMP does not have a process in place to remove wrongful conviction records.

47. As with pardons, the removal of records related to the wrongfully convicted is important to Canadians so their opportunities to get a job, travel, study or volunteer are not diminished.

48. RECOMMENDATION

To mitigate the risk of an unlawful or inappropriate disclosure, the RCMP should implement processes to remove access to the required records related to pardoned offences and wrongful convictions from the PROS database.

RCMP response:

The RCMP will immediately implement a process and the necessary technology solution to enable the sequestering of information related to individuals who have been granted a pardon. The RCMP will also amend the PROS standard operating procedure on Sequestering Information Other Than Pardons *to include instructions for the processing of records of wrongful conviction.*

There is no active review of user accounts

49. Access controls are important tools that determine who has access to what data and what actions they can perform. These actions include who may create, read, update or delete data records. We examined the access controls the RCMP has put in place to ensure the personal information contained within PROS is adequately protected.

50. We found that the RCMP has role-based access controls in place for the PROS database. Access levels are based on an individual's current job requirements. However, we also found that, as users of PROS move between jobs, their access rights are not always updated or disabled in a timely fashion.

51. The RCMP's PROS policy requires that a user's access be revoked when no longer required or after 14 months of inactivity. However, during our examination we noted there were over 1,000 users with active accounts who had not accessed PROS in 14 months or longer. The RCMP was unable to readily produce an up-to-date and accurate report of users and the status of their accounts.

52. Had the RCMP performed regular reviews of user activity, these accounts would have been disabled. There is a risk when users who are no longer authorized to access PROS retain their access. Without regular access reviews, unauthorized access may not be discovered for a long period of time.

53. RECOMMENDATION

The RCMP should regularly review the status of PROS user accounts and disable access when no longer required to perform job functions.

RCMP response:

The RCMP will take immediate steps to rectify this situation and will also examine its current training practice for employees who carry out the review of PROS user accounts.

54. **The ability to review user actions is limited.** We examined the transaction-logging capabilities of the PROS system to see if the RCMP could review reported incidents of misuse by a user. We found that PROS is able to track a user's actions in audit logs. The information recorded includes details on which records were viewed and any modifications made.

55. The RCMP informed us that if misuse by a user is suspected, the level of effort involved to consolidate and review the audit logs limits the ability to investigate. While an automated audit log review tool is available within PROS, it has not been implemented. Without this function, extracting details of a user's activity is highly labour intensive. As a result, it is difficult for the RCMP to investigate reported misuse of the system.

56. RECOMMENDATION

To aid in the investigation of unauthorized access of personal information within PROS, the RCMP should enable the audit log review tool.

RCMP response:

The RCMP will proceed immediately to enable the Audit Log Viewer tool as an efficient method to consolidate and review the audit logs.

Compliance with policies governing use of personal information is not systematically reviewed

57. In addition to the RCMP, there are 23 police partner agencies that rely on the use of the PROS system to manage their operational records. We examined the RCMP's policies and procedures governing the use of PROS, the MOUs between the RCMP and the police partner agencies and how the RCMP ensures these agencies are in compliance with the terms and conditions of these agreements.

58. We found that the RCMP has established policies and procedures to ensure that its use of PROS respects the principles for use of personal information set out in the *Privacy Act*. The RCMP sets out conditions of use in MOUs with all police partner agencies to ensure that the system is used in accordance with these policies and procedures.

59. The MOUs include terms on the acceptable use and sharing of the information contained in PROS, security provisions, training requirements, breach-reporting procedures and protocols to ensure the information contained in PROS is used for legitimate law enforcement purposes.

60. The MOUs remain in effect for five years from the date of signing, unless terminated. Reasons for termination include unauthorized use and disclosure, any breach of security policies or regulations or breach of RCMP PROS policy.

61. When we reviewed the MOUs, we found there are provisions that allow the RCMP to conduct audits of the agency to ensure compliance with the governing terms and conditions. The RCMP has the right to monitor the use of its networks, including use by specific employees, and to periodically conduct security reviews through on-site visits to police partner agencies. Audits of the use of PROS are important as they provide the RCMP with assurances that users are complying with procedures governing the use of the personal information contained in PROS.

62. The RCMP was unable to demonstrate that it systematically undertakes reviews of police partner agencies to ensure that personal information contained in PROS is used in accordance with the governing terms and conditions. A limited number of audits have been undertaken. For example, all police partner agencies in Alberta have been audited, whereas in Nova Scotia only a limited number were audited, and none at all were audited in Prince Edward Island. Further, the RCMP was unable to demonstrate that it systematically undertakes such reviews of its own users.

63. RECOMMENDATION

The RCMP should adopt a consistent and regular review process that provides assurances that all users are complying with the policies and procedures governing the use of the personal information contained in PROS.

RCMP response:

The RCMP will immediately review its existing audit process, and make amendments where necessary, to ensure that both internal and external users of PROS are subject to reviews.

Conclusion

64. The RCMP has developed and implemented policies and procedures to protect the personal information of Canadians accessed from the CPIC database. Although some privacy breaches do occur, they are relatively rare and mechanisms are in place to investigate them, and action is taken upon the results of those investigations. The RCMP had established MOUs governing the use of CPIC by agencies that have limited law enforcement powers or roles complementary to law enforcement. However, the RCMP had yet to formally establish MOUs with approximately 25 percent of the police agencies that access CPIC.

65. Regular audits are performed that examine security screening of personnel, security at the CPIC terminal and/or interface site and to ensure that policy and guidelines in the CPIC reference manual are adhered to by all agencies, including the RCMP. This monitoring regime ensures all users are compliant with the privacy principles outlined in CPIC policy.

66. The RCMP has developed policies and standard operating procedures that set out how long information may be retained before the information must be sequestered or deleted from PROS. However, personal information is being retained longer than required, in contravention of the *Privacy Act*. Further, the RCMP has no process for the removal of access to records related to pardoned offences or records related to wrongful convictions. The removal of access to records relating to pardons and the wrongfully convicted is important to Canadians so they will have the same opportunities to get a job, travel, study or volunteer as any other Canadian.

67. There is no active review of PROS user accounts. While the RCMP's PROS policy requires that a user's access be revoked when no longer required to perform their job functions or after a period of inactivity, we noted there were over 1,000 users who had not accessed PROS in 14 months or longer whose accounts were still active. Further, the ability to review user activity on PROS is cumbersome and hinders effective investigation of reported misuse.

68. The RCMP was unable to demonstrate that it systematically undertakes reviews of PROS users to ensure personal information contained in PROS is used in accordance with the governing policies.

69. The RCMP is adequately managing the personal information contained in CPIC. However, the RCMP should set a clear timeframe for establishing MOUs that include privacy provisions for all entities.

70. The RCMP needs to improve how the personal information contained in the PROS database is managed. The RCMP needs to purge data from PROS, implement processes to remove access to records related to pardoned offences and wrongful convictions, regularly review the status of PROS user accounts and disable access when no longer required to perform job functions, enable the PROS audit log review tool and adopt a consistent and regular review process that provides assurances that all users are complying with the policies and procedures governing the use of the personal information contained in PROS.

About the Audit

AUTHORITY

Section 37 of the *Privacy Act* empowers the Privacy Commissioner to examine the personal information-handling practices of federal government institutions.

OBJECTIVE

The audit objective was to determine whether the RCMP is adequately managing the personal information contained in the CPIC and PROS databases.

CRITERIA

Audit criteria are derived from the *Privacy Act*. Supporting information technology (IT) controls were assessed using selected criteria from the Control Objectives for Information and Related Technology (CobIT), an industry-standard set of best practices for IT management, and relevant Government of Canada policies and standards.

We expected to find that the RCMP:

- had established policies and procedures to govern the access and use of CPIC;
- ensures that use of CPIC is monitored for compliance with the terms and conditions of use;
- had established policies and procedures to remove personal information contained in PROS that is no longer required;
- is adequately managing access to PROS; and
- ensures that the use of PROS is monitored for compliance with RCMP policies and procedures to protect personal information.

SCOPE AND APPROACH

We examined the policies, systems, administrative controls and safeguards implemented by the RCMP for CPIC and PROS governing the use, disclosure, retention and disposal/destruction of personal information under the *Privacy Act*.

Audit evidence was obtained by examining the various standard operating procedures, agreements, process flow documents, record retention schedules, program documentation, audit reports, files and application controls. We also reviewed the user access controls and system architecture of both CPIC and PROS, and requested briefings, demonstrations and walk-throughs in support of our audit examination work.

We did not examine how the information in these databases influenced decisions as part of the day-to-day operations of the RCMP. Further, the audit did not look at the safeguards put in place by users of CPIC and PROS other than the RCMP.

The audit work was substantially completed on March 31, 2011.

STANDARDS

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

AUDIT TEAM

Director General: Steven Morgan

Sylvie Gallo Daccash
Anne Overton
Bill Wilson

Appendix: List of Recommendations

1. RECOMMENDATION

The CPI Centre should set a clear timeframe for establishing MOUs, which include privacy provisions with all entities.

RCMP response:

The CPI Centre is currently and actively in negotiation with the final 25 percent of the agencies that have yet to sign an MOU as directed by the Deputy Commissioner, Policing Support Services in November 2010. As expected, a template approach to MOUs does not necessarily apply to all cases and differences are being discussed in order to have MOUs in place by March 31, 2012.

2. RECOMMENDATION

The RCMP should purge the required data from PROS so that it is in compliance with the *Privacy Act.*

RCMP response:

The RCMP agrees and will take immediate steps to rectify this situation.

3. RECOMMENDATION

To mitigate the risk of an unlawful or inappropriate disclosure, the RCMP should implement processes to remove access to the required records related to pardoned offences and wrongful convictions from the PROS database.

RCMP response:

The RCMP will immediately implement a process and the necessary technology solution to enable the sequestering of information related to individuals who have been granted a pardon. The RCMP will also amend the PROS standard operating procedure on *Sequestering Information Other Than Pardons* to include instructions for the processing of records of wrongful conviction.

4. RECOMMENDATION

The RCMP should regularly review the status of PROS user accounts and disable access when no longer required to perform job functions.

RCMP response:

The RCMP will take immediate steps to rectify this situation and will also examine its current training practice for employees who carry out the review of PROS user accounts.

5. RECOMMENDATION

To aid in the investigation of unauthorized access of personal information within PROS, the RCMP should enable the audit log review tool.

RCMP response:

The RCMP will proceed immediately to enable the Audit Log Viewer tool as an efficient method to consolidate and review the audit logs.

6. RECOMMENDATION

The RCMP should adopt a consistent and regular review process that provides assurances that all users are complying with the policies and procedures governing the use of the personal information contained in PROS.

RCMP response:

The RCMP will immediately review its existing audit process, and make amendments where necessary, to ensure that both internal and external users of PROS are subject to reviews.